Guide to Understanding FedRAMP

Version 1.2

April 22, 2013

Executive Summary

This document provides helpful hints and guidance to make it easier to understand FedRAMP's requirements. The primary purpose of this document is to act as an aid for Cloud Service Providers and Third-Party Assessment Organizations (3PAOs) to get through the security assessment process quickly. The FedRAMP website can be found at www.fedramp.gov and information found in this document is consistent with the program described on the website. The FedRAMP program supports the U.S. government's mandate that all U.S. federal information systems comply with the Federal Information Security Management Act of 2002 (FISMA).

Document Revision History

Date	Page(s)	Description	Author
6/6/2012	All	Version 1.0	FedRAMP Office
10/15/2012	pp. 38-39	Added § 3.10.3, 3.10.4, and 3.10.5. (PE-2, PE-3, PE-4)	FedRAMP Office
10/26/2012	p. 36	Table number revised	FedRAMP Office
10/26/2012	p. 46	Table number revised	FedRAMP Office
10/26/2012	p. 49	Table number revised	FedRAMP Office
11/14/2012	p. 20	Added § 3.9, all other sections past §3.9 renumbered	FedRAMP Office
11/14/2012	p. 13	§1.5 revised	FedRAMP Office
11/14/2012	p. 33	§3.10.4.2 revised	FedRAMP Office
02/04/13	p. 40	Added §3.11.6, 3.11.7, 3.11.8	FedRAMP Office
03/04/13	p. 14	§2.2.4 revised to change 3PAO scans to annual	FedRAMP Office
03/04/13	p. 13	Updated Figure 2-1	FedRAMP Office
03/04/13	p. 38	Added new §3.11.3	FedRAMP Office
03/25/2013	p. 18	§3.7 revised	FedRAMP Office
03/25/2013	Various	§1.4 revised; §2.2 revised; §2.2.2 revised; added new §3.12 SI-5; added Figures 3-1 and 3-23; added new §3.11.15 SC-13(1); §3.9 revised; §3.15 revised, §5.2 revised.	FedRAMP Office
4/22/2013	Varioius	Minor updates to fix misnumbered headings and tables: §1.4; §3.15; §3.10.2; §3.10.4; Table of Contents, List of Tables; List of Figures.	FedRAMP Office

Table of Contents

List of Tables

List of Figures

ABOUT THIS DOCUMENT

This document has been developed to provide guidance on how to participate in and understand the FedRAMP program.

WHO SHOULD USE THIS DOCUMENT?

This document is intended to be used by service CSPs, 3PAOs, government contractors working on FedRAMP projects, government employees working on FedRAMP projects, and any outside organizations that want to make use of the FedRAMP assessment process.

HOW THIS DOCUMENT IS ORGANIZED

This document is divided into five sections. Most sections include subsections.

Section 1 provides an introduction and overview of FedRAMP.

Section 2 provides instructions for third-party assessment organizations.

Section 3 provides instructions for cloud service providers on requirements.

Section 4 provides information to cloud service providers on how to maintain their authorization.

Section 5 provides general guidance on document formatting.

CONVENTIONS USED IN THIS DOCUMENT

This document uses the following typographical conventions:

Italic

Italics are used for email addresses, security control assignments parameters, and formal document names.

Italic blue in a box

Italic blue text in a blue box indicates instructions to the individual filling out the template.

> *Instruction: This is an instruction to the individual filling out of the template.*

Bold

Bold text indicates a parameter or an additional requirement.

`Constant width`

Constant width text is used for text that is representative of characters that would show up on a computer screen.

Notes

Notes are found between parallel lines and include additional information that may be helpful to the users of this template.

Note: This is a note.

Sans Serif

Sans Serif text is used for tables, table captions, figure captions, and table of contents.

Sans Serif Gray

Sans Serif gray text is used for examples.

Tips

Tips include information designed to help simplify the process.

💡 **Tip:** This is a tip.

HOW TO CONTACT US

If you have questions about FedRAMP or this document, write to:

info@fedramp.gov

For more information about the FedRAMP project, please visit the website at:

http://www.fedramp.gov.

1. FEDRAMP INTRODUCTION

The FedRAMP program supports the U.S. government's objective to enable U.S. federal agencies to use managed service providers that enable cloud computing capabilities. The program is designed to comply with the Federal Information Security Management Act of 2002 (FISMA). This document includes guidance on how cloud service providers can meet FISMA requirements to obtain a FedRAMP Provisional Authorization.

1.1 APPLICABLE LAWS AND REGULATIONS

The following laws and regulations are applicable to the FedRAMP program:

- Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
- E-Authentication Guidance for Federal Agencies [OMB M-04-04]
- Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
- Freedom of Information Act As Amended in 2002 [PL 104-232, 5 USC 552]
- Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
- Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7]
- Internal Control Systems [OMB Circular A-123]
- Management of Federal Information Resources [OMB Circular A-130]
- Management's Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
- Privacy Act of 1974 as amended [5 USC 552a]
- Protection of Sensitive Agency Information [OMB M-06-16]
- Records Management by Federal Agencies [44 USC 31]
- Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
- Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]

1.2 APPLICABLE STANDARDS AND GUIDANCE

The following standards and guidance are applicable to the FedRAMP program:

- A NIST Definition of Cloud Computing [NIST SP 800-145]
- Computer Security Incident Handling Guide [NIST SP 800—61, Revision 1]
- Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
- Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]
- Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53A]
- Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18,

Revision 1]

- Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]
- Guide for Mapping Types of Information and Information Systems to Security Categories [NISP SP 800-60, Revision 1]
- Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]
- Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
- Managing Information Security Risk [NIST SP 800-39]
- Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
- Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-1]
- Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 3]
- Risk Management Guide for Information Technology Systems [NIST SP 800-30]
- Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
- Security Requirements for Cryptographic Modules [FIPS Publication 140-2]
- Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
- Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]

1.3 FEDRAMP GOVERNANCE

FedRAMP is governed by a Joint Authorization Board (JAB) that consists of representatives from the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Department of Defense (DoD). The FedRAMP program is endorsed by the U.S. government's CIO Council including the Information Security and Identity Management Committee (ISIMC). The ISIMC collaborates on identifying high-priority security and identity management initiatives and developing recommendations for policies, procedures, and standards to address those initiatives.

1.4 OVERVIEW OF THE FEDRAMP PROCESS

FedRAMP provides a streamlined avenue for U.S. federal agencies to make use of cloud service provider platforms and offerings. The FedRAMP program provides an avenue for CSPs to obtain a Provisional Authorization after undergoing a third-party interdependent security assessment that has been reviewed by the JAB. By assessing security controls on candidate platforms, and providing Provisional Authorizations on platforms that have acceptable risk, FedRAMP enables federal agencies to forego the security assessment process for a multitude of known security controls. An overview of the FedRAMP process is portrayed in Figure 1-1.

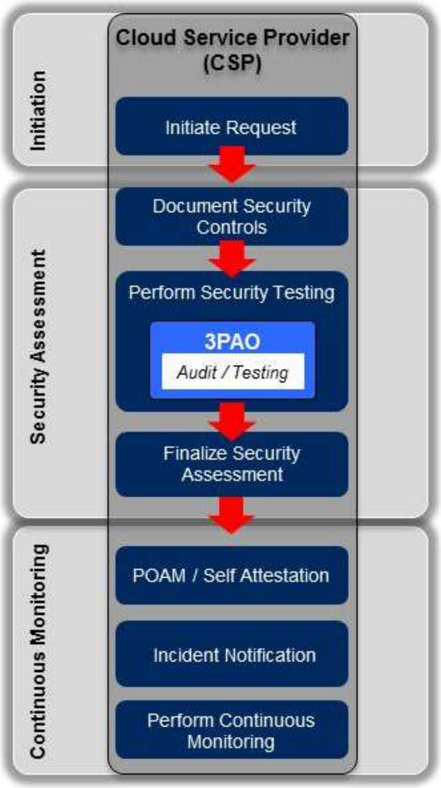


Figure 1-1. FedRAMP Process

The independent assessment is paid for by the CSP and must be performed in accordance with FedRAMP assessment procedures. CSPs should select a 3PAO from the list of accredited 3PAOs which is published at the following URL:

http://www.gsa.gov/portal/content/131991

When an agency leverages a Provisional Authorization, that agency will still need to address a subset of security controls within their own agency for the controls not addressed by the Provisional Authorization. Refer to the use cases in Section 3.10.2 for more information on how agencies layer security controls on top of cloud services.

After a Provisional Authorization is granted, CSPs must maintain their compliance by performing a variety of continuous monitoring tasks as described in the *FedRAMP Continuous Monitoring and Strategy Guide*.

2. GUIDELINES FOR THIRD-PARTY ASSESSMENT ORGANIZATIONS

3PAOs will need to provide an independent assessment in accordance with the FedRAMP program guidelines. The intended audience for this section is 3PAOs.

2.1. HOW TO BECOME A 3PAO

An organization must fill out an application and apply to become an accredited 3PAOs. The application requires that prospective 3PAOs demonstrate competencies in assessing security controls. Additionally, prospective 3PAOs must have an operational Quality Management System in place at their organization and must demonstrate knowledge of standard conformity assessment processes. See www.fedramp.gov for the application and related materials.

2.2. SECURITY TESTING

It is a goal of the FedRAMP program for all CSP systems to be assessed equally and according to the same security baseline controls appropriate for the designated sensitivity category. In light of this objective, templates have been provided to standardize the assessment process. The templates designed for 3PAOs to fill out are the *Security Assessment Test Cases*, the *Security Assessment Plan* (SAP) template, and the *Security Assessment Re*port (SAR) template.

2.2.1 Security Assessment Plan (SAP) Template

The purpose of the SAP template is to describe the security testing plan. You should meet with the CSP and discuss the test engagement before developing the SAP, and again prior to finalizing the SAP. If 3PAOs have any questions on security testing they should contact the FedRAMP ISSO. The 3PAO should submit the final SAP to both the CSP and FedRAMP ISSO prior to starting to test. The ISSO will review the SAP and give the go ahead to start testing after obtaining approval from the JAB. The SAP template is available on www.fedramp.gov.

2.2.2 Security Test Test Cases

The *Security Assessment Test Cases* are based on NIST SP 800-53A. There are some FedRAMP test cases that are above and beyond those found in NIST SP 800-53A. Some of the test cases are currently unpublished by NIST and are not available on the NIST website where test cases are published (http://csrc.nist.gov/groups/SMA/fisma/assessment-cases.html).

2.2.3 Security Assessment Report (SAR) Template

The *Security Assessment Report* is the final report written by the 3PAO to detail the independent security assessment done on the CSP candidate information system. The FedRAMP program provides a *Security Assessment Report* template and all 3PAOs are required to use this template to report their findings. The SAR template is available on www.fedramp.gov.

2.2.4 Running Scans

As part of the security testing, automated scans are required. On large implementations, a subset of all representative hosts and device types should be scanned using full authentication. The advantage of running scans as fully authenticated privileged users is that the scanner can access the registry, file attributes, installed packages, and patch levels. Account credentials for the authenticated scans should use login IDs and user roles that offers the greatest possible privileges for the system being scanned (e.g. root, administrator).

The use of non-authenticated scans can assist in vulnerability severity determinations and in prioritizing remediation efforts since in a non-authenticated scan vulnerabilities are seen from the point of an attacker/intruder. Non-authenticated scans can be used in addition to fully authenticated scans if the information from these scans helps to determine the risk exposure. However, non-authenticated scans are not required by FedRAMP.

3PAOs do not need to run source code scans. However, if a CSP writes original source code that is built into their service offering, the CSP is required to perform source code scanning to satisfy control SA-11(1). If the CSP service offering uses CSP developed original code, the 3PAO should ask the CSP to provide the results of a source code analysis report (from a code analysis scanner) for the current release.

Tip: An authenticated scan is sometimes referred to as a credentialed scan or a host-based scan.

All scan results should be sent to the government FedRAMP ISSO at the same time the SAR is provided. CSP systems must be scanned annually by a 3PAO in order to maintain their authorization. The scan does not have to be performed by the same 3PAO that performed the scan previously.

3. GUIDELINES FOR CLOUD SERVICE PROVIDERS

This section is provided to assist CSPs in understanding how to satisfy requirements for the FedRAMP program. The intended audience for this section is CSP staff.

3.1 BEFORE YOU BEGIN

In prior cloud FISMA compliance projects, certain controls have proven to be challenging for service providers to meet. Before you decide to initiate a request to participate in FedRAMP, go through the checklist in Table 3-1 and make sure that you are truly able to meet these requirements. Consult with your legal team and technical staff (e.g. systems administrators, database administrators, network engineers etc.) to determine if you have the right controls in place and have the ability to manage them.

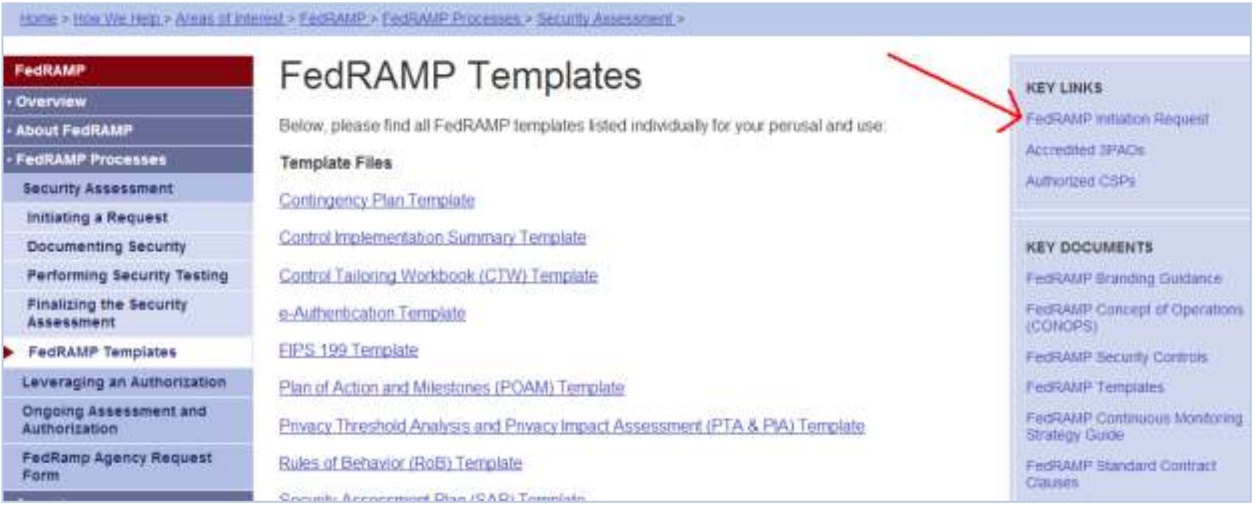
Table 3-1. Preparation Checklist

Checklist		Description
□	1	You have the ability to process electronic discovery and litigation holds
□	2	You have the ability to clearly define and describe your system boundaries
□	3	You can identify customer responsibilities and what they must do to implement controls

Checklist		Description
□	4	System provides identification & 2-factor authentication for network access to privileged accounts
□	5	System provides identification & 2-factor authentication for network access to non-privileged accounts
□	6	System provides identification & 2-factor authentication for local access to privileged accounts
□	7	You can perform code analysis scans for code written in-house (non-COTS products)
□	8	You have boundary protections with logical and physical isolation of assets
□	9	You have the ability to remediate high risk issues within 30 days, medium risk within 90 days
□	10	You can provide an inventory and configuration build standards for all devices
□	11	System has safeguards to prevent unauthorized information transfer via shared resources
□	12	Cryptographic safeguards preserve confidentiality and integrity of data during transmission

3.2 INITIATING THE PROCESS

Cloud service providers (CSPs) should initiate their desire to participate in FedRAMP by submitting an *FedRAMP Initiation Request* form. This is a web based form and is found on the FedRAMP website. This form advises the FedRAMP Program Management Office (PMO), and the JAB of the intent to obtain a FedRAMP Provisional Authorization.


Home > How We Help > Areas of Interest > FedRAMP > FedRAMP Processes > Security Assessment >
FedRAMP
• Overview
• About FedRAMP
• FedRAMP Processes
Security Assessment
Initiating a Request
Documenting Security
Performing Security Testing
Finalizing the Security Assessment
FedRAMP Templates
Leveraging an Authorization
Ongoing Assessment and Authorization
FedRamp Agency Request Form

FedRAMP Templates

Below, please find all FedRAMP templates listed individually for your perusal and use:

Template Files

Contingency Plan Template

Control Implementation Summary Template

Control Tailoring Workbook (CTW) Template

e-Authentication Template

FIPS 199 Template

Plan of Action and Milestones (POAM) Template

Privacy Threshold Analysis and Privacy Impact Assessment (PTA & PIA) Template

Rules of Behavior (RoB) Template

Security Assessment Plan (SAP) Template

KEY LINKS

FedRAMP Initiation Request

Accredited 3PAOs

Authorized CSPs

KEY DOCUMENTS

FedRAMP Branding Guidance

FedRAMP Concept of Operations (CONOPS)

FedRAMP Security Controls

FedRAMP Templates

FedRAMP Continuous Monitoring Strategy Guide

FedRAMP Standard Contract Clauses

Figure 3-1. FedRAMP Initiation Request Form

On the *FedRAMP Initiation Request* form, you will need to provide a categorization of your systems and indicate the information types based upon NIST SP 800-60 V2 guidelines. CSPs should use the data type sensitivity categorization to select which control baseline to implement – Low or Moderate. (High sensitivity categorizations are currently not part of the FedRAMP program.) The FedRAMP PMO will place your *FedRAMP Initiation Request* form in a queue and assign a timeframe for processing. You will be notified of a scheduled conference call with the FedRAMP PMO and the conference call will signify the security assessment process start and kick-off.

While you are waiting to hear back from the FedRAMP PMO, you should start researching which 3PAO that you plan on using for the security assessment. FedRAMP accredited 3PAOs are listed on the FedRAMP website.

3.3 AFTER ACCEPTANCE INTO THE FEDRAMP PROGRAM

After your CSP candidate system has been accepted into the FedRAMP program, there are certain documents that you will be required to submit. FedRAMP has created templates for these documents which the CSP should edit and modify based on the security controls implemented in the candidate system. All templates are available on the FedRAMP website. Guidance on how to fill out the various templates and how to develop the required documents are described in the sections that follow.

3.4 FIPS 199 TEMPLATE

The FIPS 199 template exists so that CSPs can categorize and record the sensitivity level of their candidate system. CSPs should use NIST SP 800-60, Revision 1, Volume 2, to select the Information Type for their candidate system. IaaS and PaaS providers should select information types from Section C.3.5 in NIST SP 800-60 Revision 1, Volume 2 and those information types are noted in Table 3-2. SaaS providers should select information types from the entire list of possible information types.

Table 3-2. Information Types for IaaS Providers

C.3.5 Information and Technology Management
C.3.5.1 System Development Information Type
C.3.5.2 Lifecycle/Change Management Information Type
C.3.5.3 System Maintenance Information Type
C.3.5.4 IT Infrastructure Maintenance Information Type
C.3.5.5 Information Security Information Type
C.3.5.6 Record Retention Information Type
C.3.5.7 Information Management Information Type
C.3.5.8 System and Network Monitoring Information Type
C.3.5.9 Information Sharing Type

The FIPS 199 analysis should be performed with respect to service provider system data only. Customer agencies will be performing a separate FIPS 199 analysis for their customer owned data hosted on the system.

3.5 E-AUTHENTICATION TEMPLATE

An e-Authentication template has been provided for the purpose of performing an e-Authentication analysis. The objective for selecting the appropriate e-Authentication level for the candidate system is so that the CSP system owner can then more easily proceed to select the right technology solution to implement the designated level. Guidance on selecting the system authentication technology solution is available in *NIST SP 800-63, Revision 1, Electronic Authentication Guidance*.

Note: NIST SP 800-63, Revision 1 can be found at the following URL: http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

You should ensure that your final e-Authentication analysis is consistent with Table 2-5 in the *System Security Plan*.

Note: Please refer to *OMB Memo M-04-04 E-Authentication Guidance for Federal Agencies* for more information on e-Authentication.

The e-Authentication template is available on www.fedramp.gov.

3.6 PRIVACY THRESHOLD ANALYSIS & PRIVACY IMPACT ASSESSMENT

All CSPs are required to fill out a *Privacy Threshold Analysis* (PTA). FedRAMP provides at PTA/PIA template and the PTA consists of four short questions designed to determine if the system qualifies as a Privacy Sensitive System. If the result of the PTA qualifies the system as a Privacy Sensitive System, then a *Privacy Impact Assessment* is also required.

Note: In accordance with NIST SP 800-144, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

CSPs should consider whether or not their security controls (for their own support staff) use PII for any authentication mechanisms (e.g. fingerprint scanners, hand scanners, iris scanners). If the CSP system will require PII from agency customers, for example to enroll users in authentication mechanisms, then the impending collection of that PII on first use by agency customers should be made known.

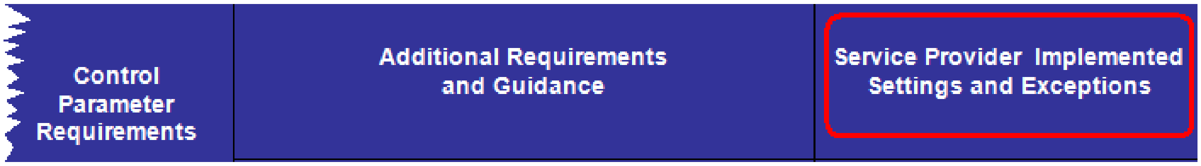
When performing the independent security assessment the 3PAO will review the PTA and/or a PIA and may make certain determinations and findings that are incorporated into the *Security Assessment Report* (SAR).

A combination PTA and PIA template is provided and is available on www.fedramp.gov.

3.7 CTW TEMPLATE

The purpose of the *Control Tailoring Workbook* (CTW) template is to summarize the exception scenarios are for the candidate service offering for prospective agency customers. This template should be filled out after the *System Security Plan* has been completed and it should be consistent with information found in the *System Security Plan*.

The right-hand most column (see Figure 3-2) in the CTW is labeled "Service Provider Implemented Settings and Exceptions". In this column CSPs should describe any setting in their candidate service offering that is different from either the stated Control Parameter Requirements or the stated Additional Requirements and Guidance. If a parameter or requirement simply does not exist in the candidate service offering, that should be noted as "not implemented". If the candidate service offering uses an alternative or compensating control, that fact should be noted with a brief explanation of how the alternative control works. If a control does not exist but is planned for future implementation, that information should be noted along with a brief explanation of how and when the control will be implemented in the future. For planned controls, an anticipated implementation date should also be noted. If your CSP candidate system meets all required security controls, settings, and parameters, the CSP should note "Meets" in the right-hand most column for the associated control.



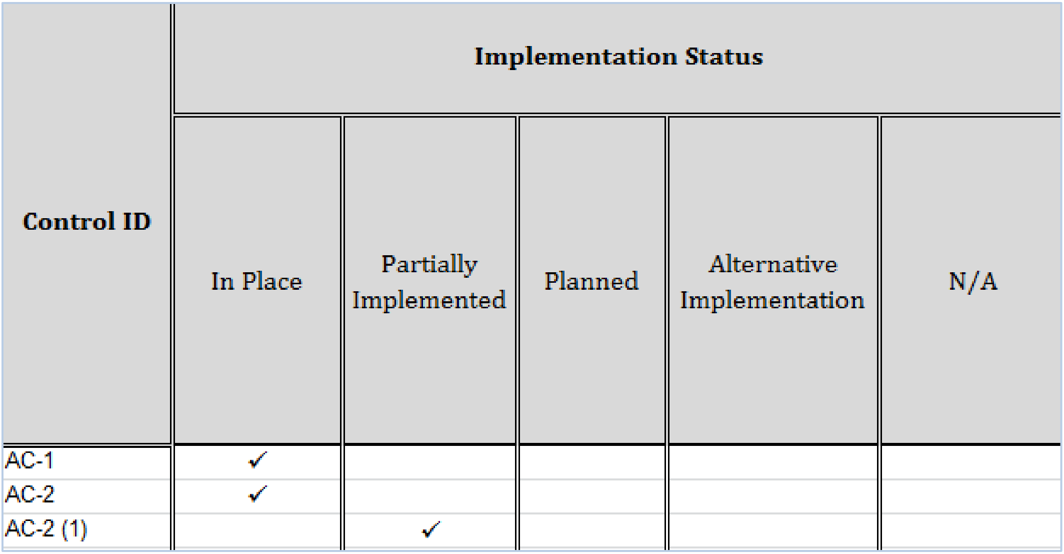
Control Parameter Requirements	Additional Requirements and Guidance	Service Provider Implemented Settings and Exceptions

Figure 3-2. Screenshot from CTW

The CTW template can be downloaded from www.fedramp.gov.

3.8 CIS TEMPLATE

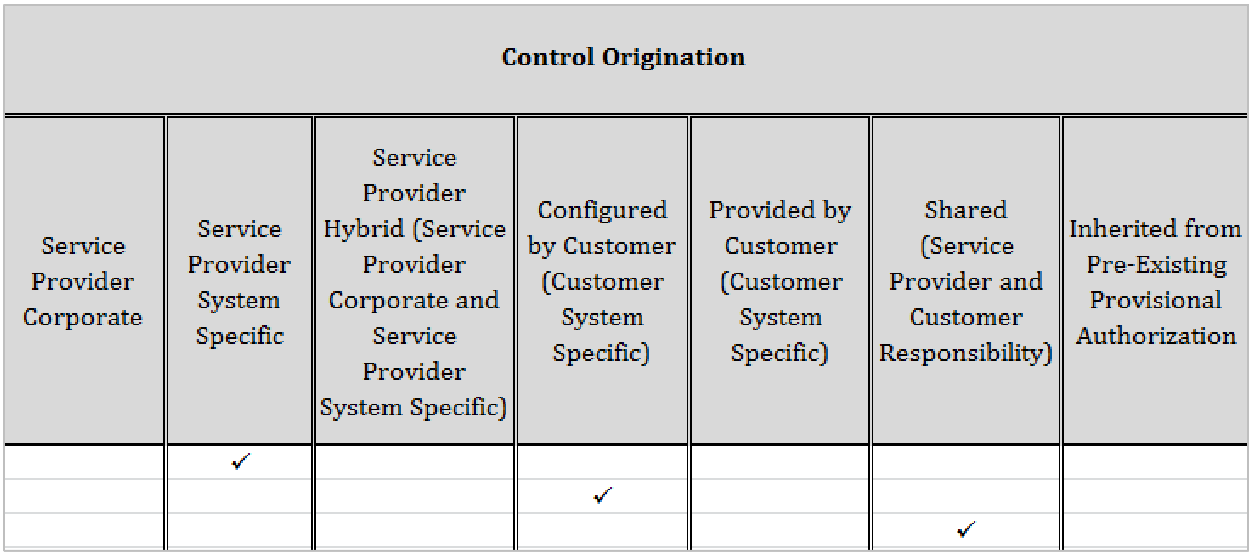
The *Control Implementation Summary* (CIS) template should be filled out to indicate the implementation status of the controls for their candidate system as illustrated in Figure 3-3.



Control ID	Implementation Status				
	In Place	Partially Implemented	Planned	Alternative Implementation	N/A
AC-1	✓				
AC-2	✓				
AC-2 (1)		✓			

Figure 3-3. Select the Implementation Status in the CIS

Additionally, CSPs need to indicate in the CIS the entity that owns the responsibility to implement and manage the control. In some cases, implementation and management of a control may require joint ownership by the CSP and the customer agency. An example of control origination selections for three different controls is illustrated in Figure 3-4.



Control Origination						
Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Service Provider Corporate and Service Provider System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Provisional Authorization
	✓					
			✓			
					✓	

Figure 3-4. Select the Control Origination Responsibility

The CIS is considered a living document and it is okay to update it throughout the development of the *System Security Plan*.

3.9 USER GUIDE

CSPs should also provide a User Guide that explains how prospective users will use the system. The User Guide should be submitted at the same time the *System Security Plan* is submitted.

3.10 COMPONENTS, BOUNDARIES, AND ARCHITECTURE

The audience for this section is CSPs; however, 3PAOs may want to review this section to better understand CSP requirements. The *System Security Plan* template is designed for you to describe how all required security controls are implemented.

3.10.1 Describing Information System Components (§ 9.2 SSP)

The information system you are describing likely has multiple components to it. Each of those components needs to be named and described in Section 9.2 of the *System Security Plan*. You may want to use component names that are already known to your company. Components may be described by a unique name (e.g. "Home Base") or by functionality (e.g. "the Hypervisor"). For example, your information system platform and offering might consist of components known as Control Tower, Front Door, Home Base, Builder Box, Holding Vault, App One and Web Wiz as illustrated in Figure 3-5.

When naming and describing the components, you should be sure that you are consistent in using these same component names throughout the entirety of your *System Security Plan* and all of the FedRAMP documents. You may avoid much confusion within your own organization if you retain component names that are already known to your organization -- that are already described in existing company documentation. If you are at any point required to supply supporting documentation, and the supporting documentation has different component names in it than what you originally provided to FedRAMP, this will create a lot of confusion and it could delay the whole FedRAMP security assessment process.

Once the FedRAMP security assessment process has started, if a component has its name changed for any reason, the Change Control Process (as described in your *Configuration Management Plan*) for the information system should capture and include a recorded history of the name change. Submitting initial documentation with one set of component names, and then submitting subsequent documents with another set of component names accompanied by an email that states "We changed the names of our components..." will not be sufficient and could cause substantial delays in your FedRAMP security assessment.

Tip: Select component names and stick to the original names.

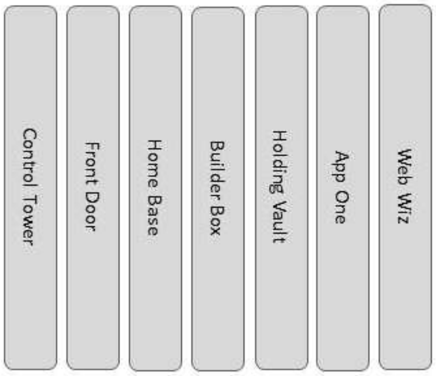


Figure 3-5. Example of Components Described by Name

Figure 3-4 illustrates software components described by unique names and Figure 3-6 illustrates software components described by functionality. Regardless of which method you use to describe your components, you will still need to include a detailed description of the functionality that each component provides to the overall system.

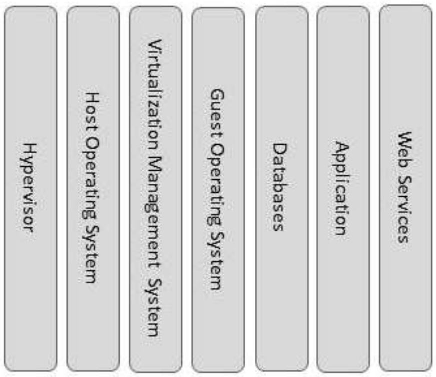


Figure 3-6. Example of Components Described by Function

3.10.2 Use Cases

There are multiple types of cloud configurations that are conceivable. The FedRAMP program does not endorse or prescribe any particular type of cloud configuration. However, for the purpose of assisting CSPs in describing the scenario that their cloud configuration represents, various use case scenarios are illustrated in the sections that follow. The uses cases presented do not constitute all possible use cases that have the potential of being built. When describing your system, you may use any of the illustrations presented, or any similar illustrations, if it helps you to more easily describe your system.

Note: For more information on cloud use cases, please consult NIST SP 500-293, U.S. Government Cloud Computing Technology Roadmap, Volume II (Draft).

3.10.2.1 Case 1: Simple IaaS

It's possible that an agency may want to use one IaaS provider with the intention of having the top layer controls (platform and application) provided by the agency. In this scenario, one FedRAMP Provisional Authorization is applicable as illustrated in Figure 3-7.

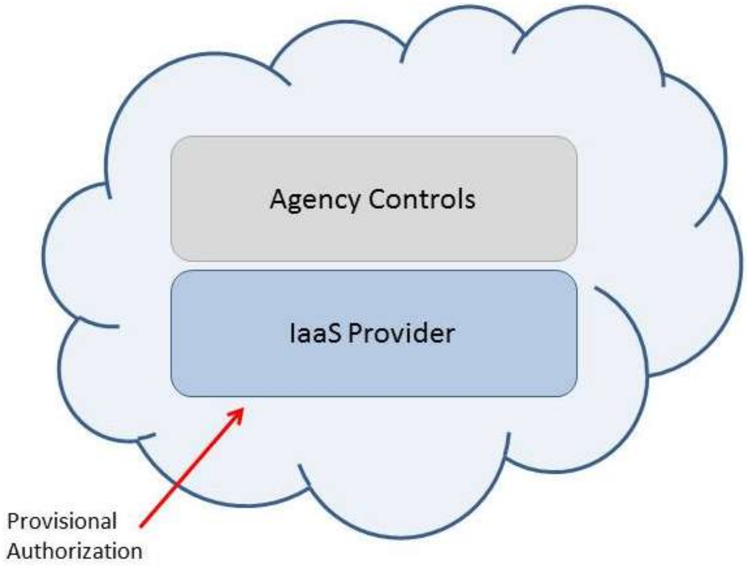


Figure 3-7. One IaaS Provider

3.10.2.2 Case 2: Simple PaaS

It's possible that an agency may want to use one provider that provides both the IaaS and PaaS layers, with the intention of having the top layer controls (application) provided by the agency. In this scenario, one FedRAMP Provisional Authorization is applicable as illustrated in Figure 3-8.

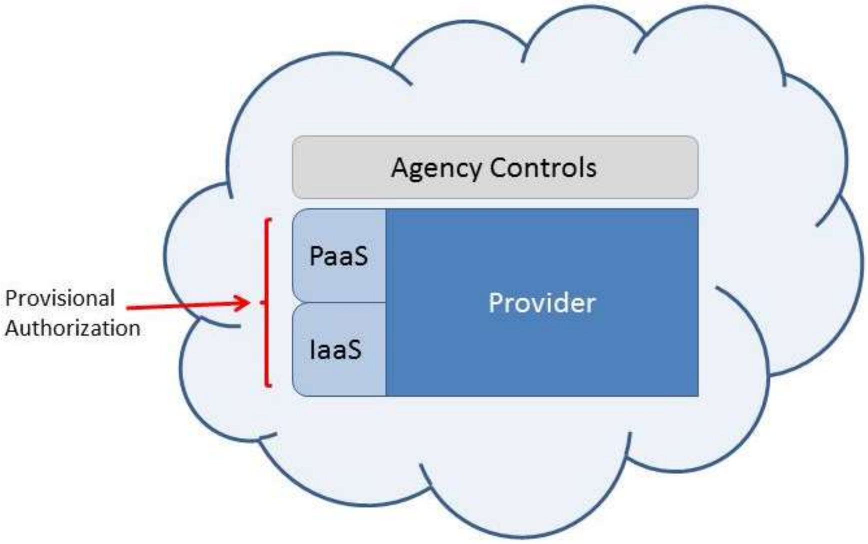


Figure 3-8. One Provider for IaaS and PaaS

3.10.2.3 Case 3: Simple SaaS

It’s possible that an agency may want to use one provider that provides the IaaS, PaaS, and SaaS layers. In this scenario, one FedRAMP Provisional Authorization is applicable as illustrated in Figure 3-9.

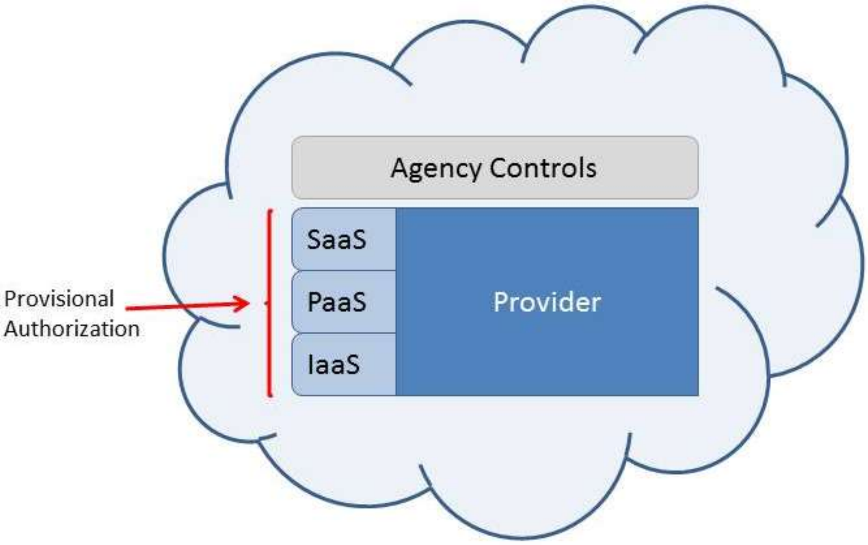


Figure 3-9. One Provider, IaaS, PaaS, and SaaS

3.10.2.4 Case 4: One Provider, Just SaaS

It’s possible that a cloud service provider may build a SaaS application that encompasses the entire stack of security controls, but does not differentiate between the PaaS and IaaS layers as illustrated in Figure 3-10. NIST SP 500-293, Volume II (Draft) states:

> *It is possible, though not necessary, that SaaS applications can be built on top of PaaS components, and PaaS components can be built on top of IaaS components.*

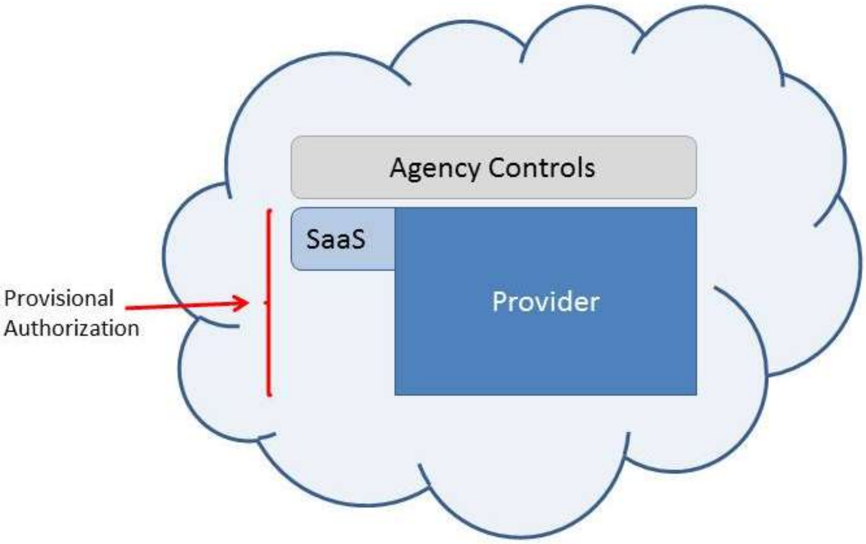


Figure 3-10. One Provider, Just SaaS

3.10.2.5 Case 5: Two Cloud Providers, IaaS and PaaS

It's possible that an agency may want to use one provider that provides IaaS and a different provider that provides the PaaS layer. In this scenario, the Paas provider is dependent on leveraging a pre-existing Provisional Authorization – from the IaaS provider. In this scenario, if the agency decides to make use of this integrated package, two different FedRAMP Provisional Authorizations are applicable as illustrated in Figure 3-11.

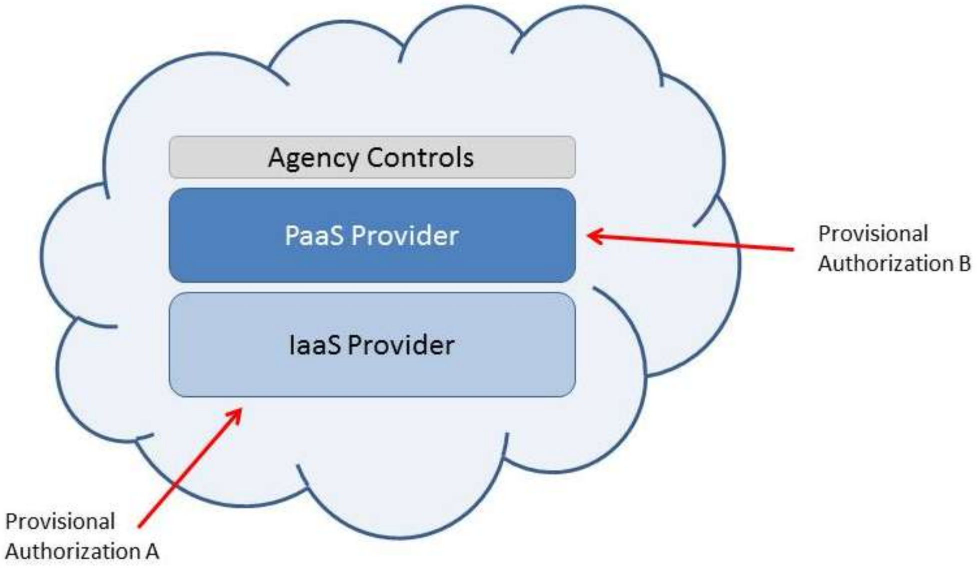


Figure 3-11. Two Providers, One IaaS and One PaaS

3.10.2.6 Case 6: Three Cloud Providers, IaaS, PaaS, and SaaS

It's possible that an agency may want to use three providers that each provide a different layer. In this scenario, the PaaS provider is dependent on leveraging a pre-existing Provisional Authorizations from the IaaS provider and the SaaS provider is dependent on leveraging a pre-existing Provisional Authorization from the PaaS provider (and indirectly the IaaS provider). In this scenario, if the agency decides to make use of this integrated package, three different FedRAMP Provisional Authorizations are applicable as illustrated in Figure 3-12.

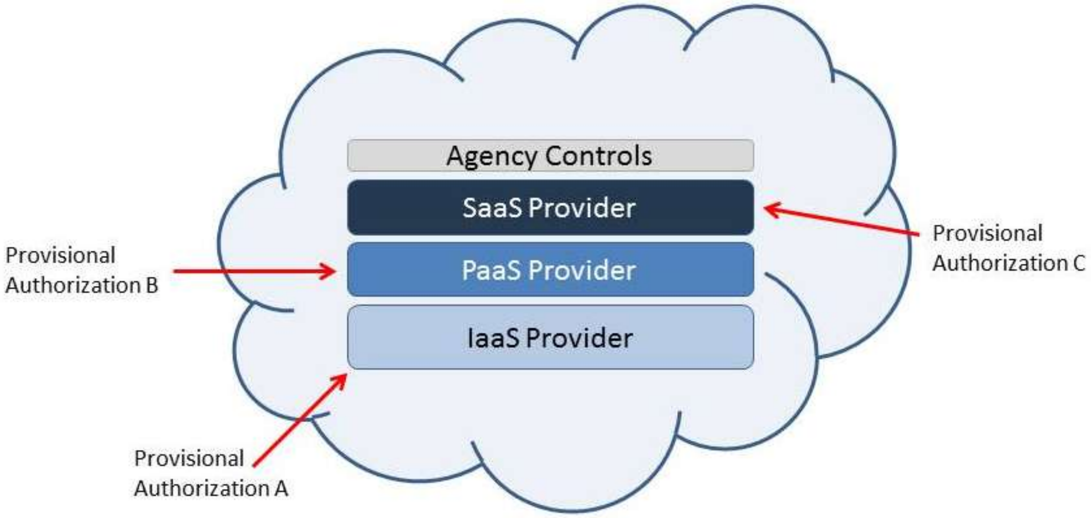

Agency Controls
SaaS Provider
PaaS Provider
IaaS Provider
Provisional Authorization C
Provisional Authorization B
Provisional Authorization A

Figure 3-12. Three Providers, One IaaS, One PaaS, and One SaaS

3.10.2.7 Case 7: Two Cloud IaaS Providers

It's possible that an agency may want to make use of two separate IaaS providers with the intention of having the top layer controls (platform and application) provided completely by the agency. In this scenario, two different FedRAMP Provisional Authorizations are applicable as illustrated in Figure 3-13.

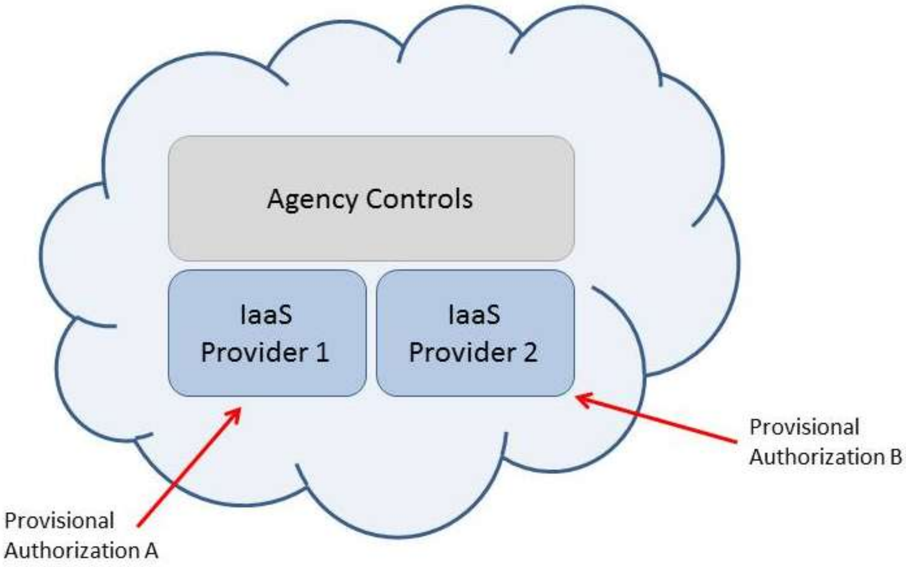


Figure 3-13. Two IaaS Providers

3.10.2.8 Case 8: Two Cloud IaaS Providers and a PaaS Provider

It's possible that a cloud implementation could make use of two separate IaaS providers and a third separate PaaS provider. In this scenario, the Paas provider is dependent on leveraging two pre-existing Provisional Authorizations – one from each of the IaaS providers. In this scenario, if the agency decides to make use of this integrated package, three different FedRAMP Provisional Authorizations are applicable as illustrated in Figure 3-14.

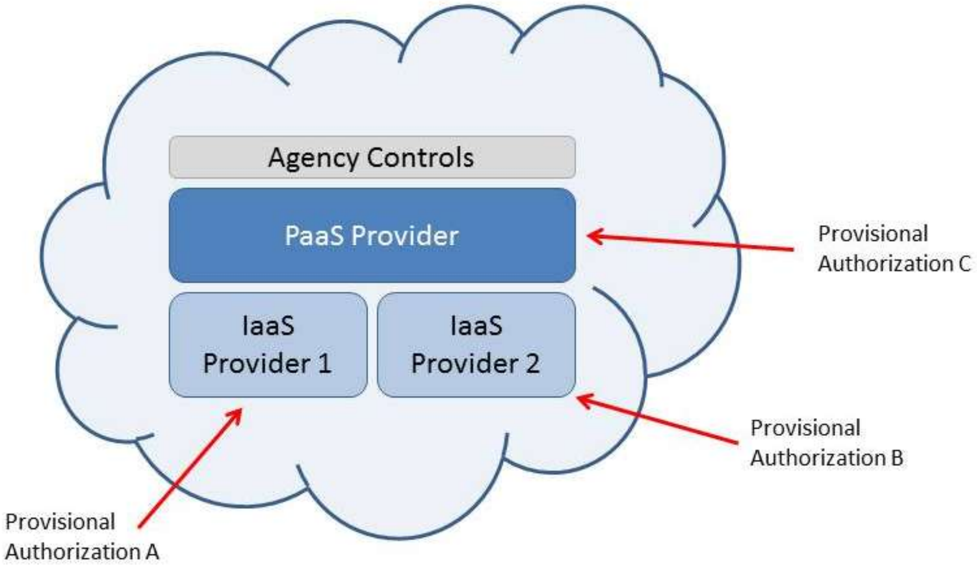

Agency Controls
PaaS Provider
IaaS Provider 1
IaaS Provider 2
Provisional Authorization C
Provisional Authorization B
Provisional Authorization A

Figure 3-14. Two IaaS and One PaaS Provider

When IaaS Provider 1 writes their *System Security Plan*, they will not indicate that they are leveraging any other Provisional Authorization. The same holds true for IaaS Provider 2. However, when the PaaS provider writes their *System Security Plan*, in Section 8.2 of the *System Security Plan*, they should indicate that they are leveraging the Provisional Authorization of both IaaS Provider 1 and IaaS Provider 2. It is anticipated that the PaaS provider will inherit controls from both IaaS providers.

3.10.2.9 Case 9: Three Cloud Providers, One IaaS and Two PaaS

It's possible that a cloud implementation could make use of one IaaS provider and two PaaS providers. In this scenario, both Paas providers are dependent on leveraging the pre-existing Provisional Authorizations from the IaaS providers. In this scenario, if the agency decides to make use of this integrated package, three different FedRAMP Provisional Authorizations are applicable as illustrated in Figure 3-15.

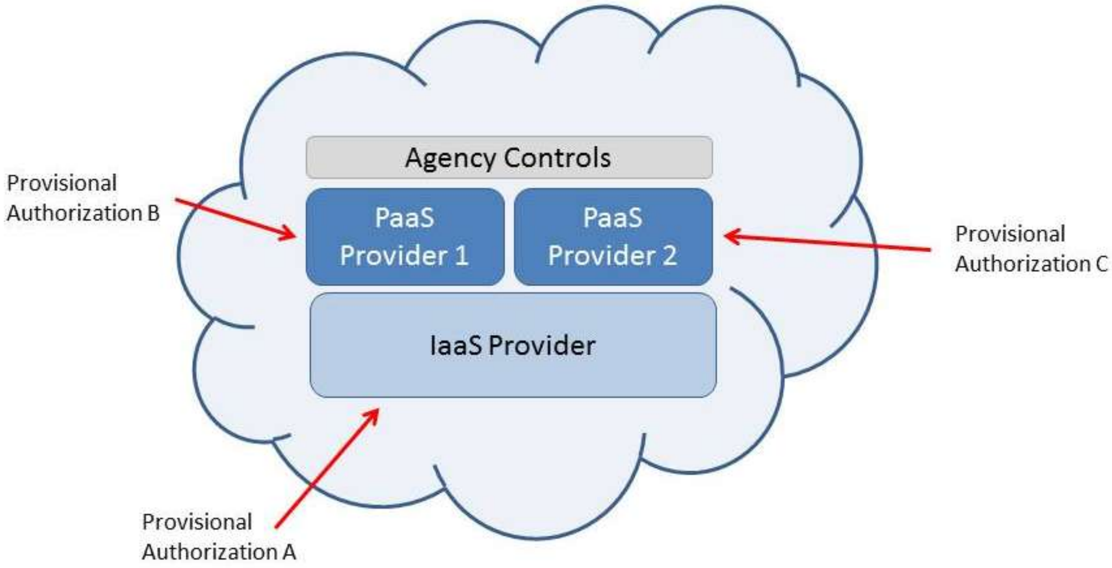

Agency Controls
PaaS Provider 1
PaaS Provider 2
IaaS Provider
Provisional Authorization B
Provisional Authorization C
Provisional Authorization A

Figure 3-15. Three Providers, One IaaS and Two PaaS

3.10.3 Discussing Virtualization

This section includes some general guidance on discussing virtualization in *System Security Plans*. CSPs use virtualization techniques that create entire systems (virtual machines or guest hosts) that are embedded inside of a traditional physical host system. There are numerous ways that virtualization can be implemented and the FedRAMP program does not make recommendations on virtualization models. There are many different virtualization products and FedRAMP does not preference one virtualization product over another. Whatever virtualization architecture model is used, CSP documentation in all aspects should be clear about which components are part of the physical host system and which components are part of virtual abstraction layers.

Note: Please refer to *NIST SP 800-125, Guide to Security for Full Virtualization Technologies* for information on types of virtualization.

Please refer to *NIST SP 800-145, The NIST Definition of Cloud Computing* for information on cloud computing architecture models.

When discussing the functionality of the different components, indicate whether the component is a standard host operating system or a guest (virtual) operating system. For each physical host that provides the capability to implement guest systems, discuss whether the virtualization technique is based on hosted virtualization or bare metal virtualization.

Guest operating systems can be deployed in several ways (i) the CSP provides a self-service menu driven control panel where customers can setup and configure their own virtual machines within a controlled environment; (ii) the CSP installs and configures unique virtual machines instances directly for the customer thereby eliminating the need for a self-service portal. When discussing administration, access control, and configuration settings of virtual machines, CSPs need to be clear about whether their service offers a self-serve solution or a CSP administered solution. The roles and authorizations associated with both of these solutions should be detailed in the *System Security Plan* (Table 9-1) User Roles and Privileges.

Not considering applications and platforms, network components can also be virtualized. If you are discussing a network component (or device) that is a virtual component, you need to be clear about the fact that the item you are discussing is virtual and not physical. Examples of virtual network components and devices are:

- Virtual Local Area Networks (VLANs)
- Virtual Ethernet Modules
- Virtual Firewalls
- Virtual Switches
- Virtual Distributed Switches
- Virtual Security Gateways
- Virtual Routers
- NAT Virtual Interfaces (NVI)

3.10.4 Discussing Boundaries (§ 9.2 in SSP)

When you are describing the boundaries of your system, it is important to accurately articulate where your cloud service layers begin and end. If you are a PaaS service provider and you are building your service on top of an IaaS service provider, you need to ensure that your security control boundaries begin where the IaaS security control boundaries end. If you are SaaS provider, you need to understand where the PaaS security control boundaries end. The security controls for an upper layer service needs to begin where the lower layer security controls end as illustrated in Figure 3-16. There are many possible configurations for layering security and FedRAMP does not make recommendations on service models.

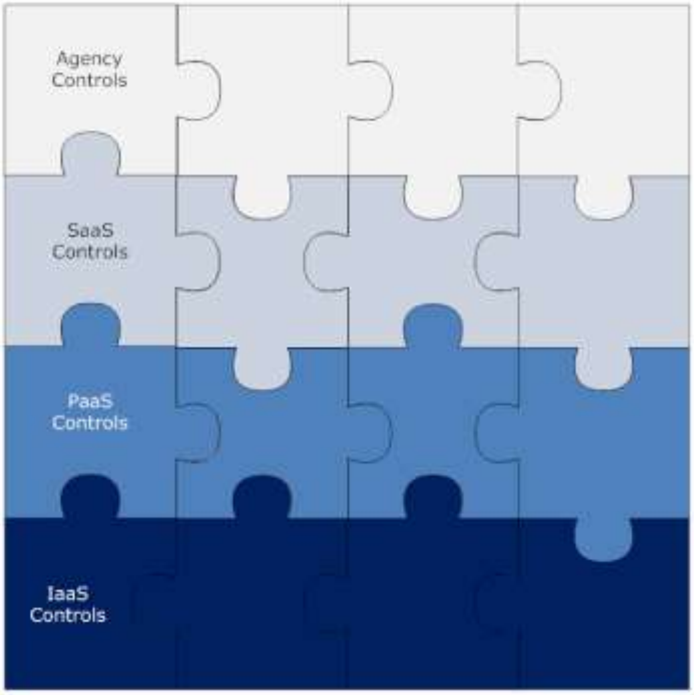


Figure 3-16. Security Controls Fitting Together

If parts of a security control boundary are not well understood, it is possible that there could be gaps in the security control boundary between the layers as illustrated in Figure 3-17.

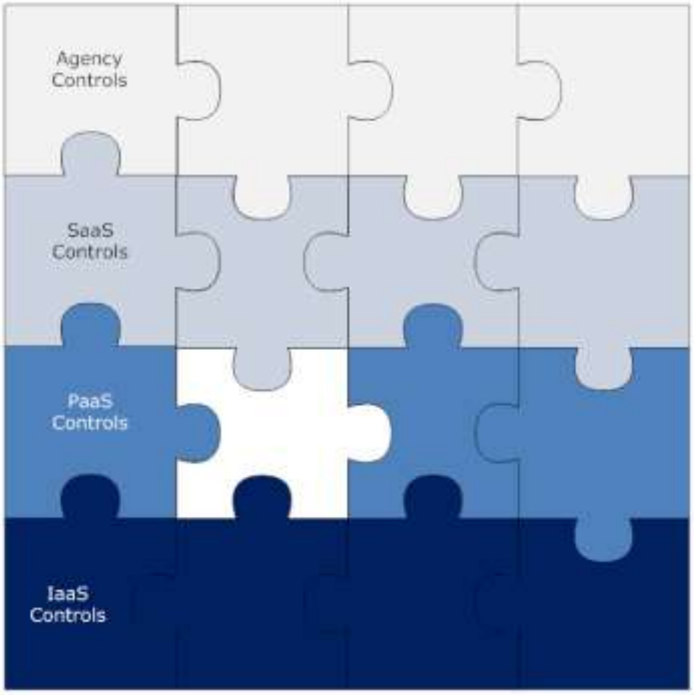


Figure 3-17. Security Control Gap

When discussing boundaries, be sure to include information on how different tenants are separated from each other in a multi-tenant environment.

Questions that you should consider when describing your boundaries are:

- Will your boundaries leverage any existing Provisional Authorizations?
- What is your definition of a tenant?
- For your service offering, will multiple tenants share the same VLAN(s)?
- Are there controls that prevent VLAN hopping?
- Do you isolate virtual machine zones on unique network segments?
- Do you use separate physical network adapters to isolate virtual machine zones?
- Is layer-2 isolation performed?
- Is isolation through traffic encapsulation used?
- Do port groups define any boundaries?
- If port groups are used, are they all in the same layer-2 domain or do they span multiple layer-2 domains?
- Do you bond multiple Network Interface Cards (NICs) together?
- How do firewalls provide isolation between tenants?
- How do router ACLs provide isolation between tenants?
- Are IPsec tunnels used to define boundaries?
- Are network filters used that control what packets are sent to or from a virtual machine?
- Are network zones used? If yes, how are zones defined?
- Will U.S. federal agencies be multi-tenanted with non-government entities?
- Do you use NAT virtual interfaces (NVI) or domain specific NAT configurations?
- How does NAT play a role in containing network traffic within the boundary?
- What kind of NAT is used? (e.g. static, dynamic, overloading, overlapping)
- Do you use NAT IP pools?
- Are geo iplocation boundaries used?
- How will you know the geographic location (City, State) where customer data is stored?
- Will it be possible for agency customers to know the geographic location (City, State) where their data is stored?

Tip: NAT can be used to do the following: allow internal users access to the Internet, allow the Internet to access devices inside the boundary, redirect TCP traffic to another port or address, allow overlapping networks to communicate, allow networks with different address schemes to communicate, allow the use of application level gateways.

3.10.4.1 Discussing Live Migrations

Live migrations of virtual machines have the potential to confuse a common understanding of the information system boundaries. Therefore, when describing boundaries, it is important to discuss the live migration strategy for the information system. Live migrations have the ability to move an entire virtual machine to another host or instead to move a virtual machine's data store (configuration file and virtual disks) to another physical host without actually moving the virtual machine. Complicating this, it is also possible to move and store a virtual machine's configuration files, and disks in separate locations. FedRAMP does not make recommendations on live migration strategies. However, whatever the live migration strategy is, FedRAMP wants to understand how live migrations are managed. IP addresses declared within the boundary must remain protected by the security controls noted in the *System Security Plan* even if the IP addresses are move around.

Questions that you should consider in your discussion on live migration are:

- Are live migrations performed manually or are they scheduled and automated?
- If live migrations are automated, what are the rules that govern the migration?

FedRAMP is interested in understanding how virtual machines are monitored and how guest systems are migrated one from physical host to another. Consider discussing how virtual machine migration and tracking can be audited through logging and event generation in Section 13.13.2 (AU-2a) of the *System Security Plan*.

3.10.4.2 Discussing Storage Components

In your description of system components, you should include information about storage components that are inside the boundary. If you are using a fiber channel storage array, insert a diagram that shows how the storage connects to the fiber channel fabric and include the switches in the diagram. An example illustration is shown in Figure 3-18.

Questions that you should consider when describing your storage components are:

- Does the system use Direct Attached Storage (DAS), Network Attached Storage (NAS), or Storage Area Networks (SANs)?
- If you use a SAN, what is used to connect hosts in a cluster (fiber channel or iSCSI)?
- Which fiber channel or iSCSI connections are considered within the boundary?
- Are different types of storage devices used on different network segments?
- Are clusters used?
- How many hosts are on a cluster and which clusters are in the boundary?
- Do the storage devices use a multipath environment?
- Are the storage devices setup to be persistent or non-persistent?

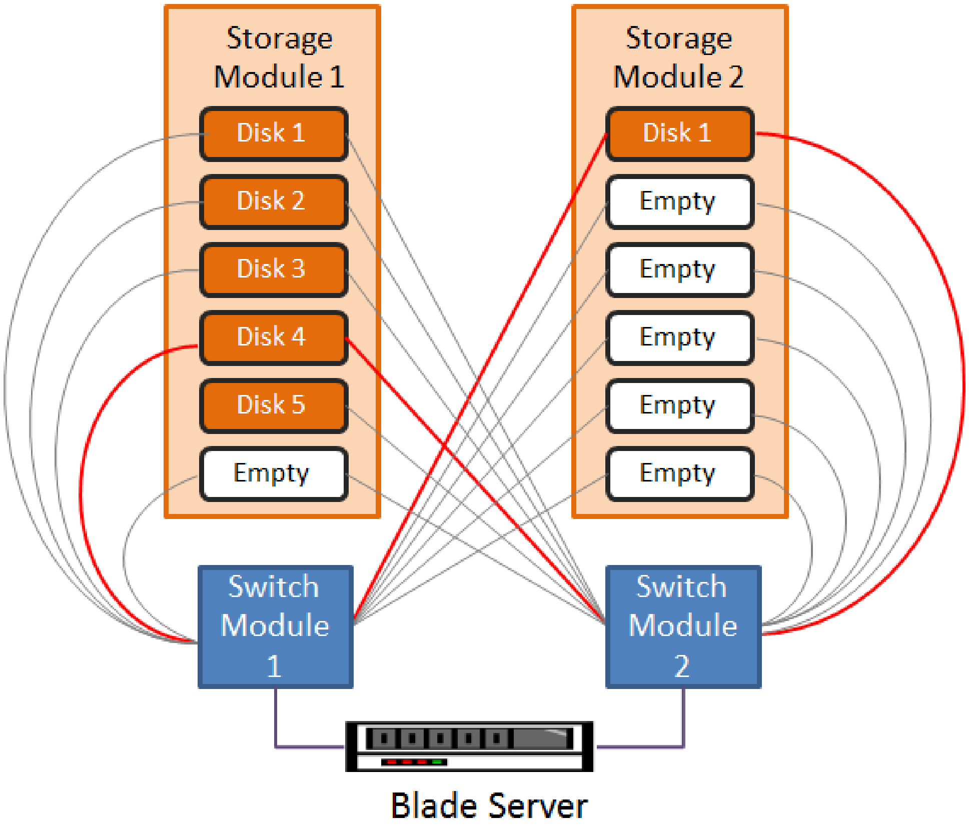
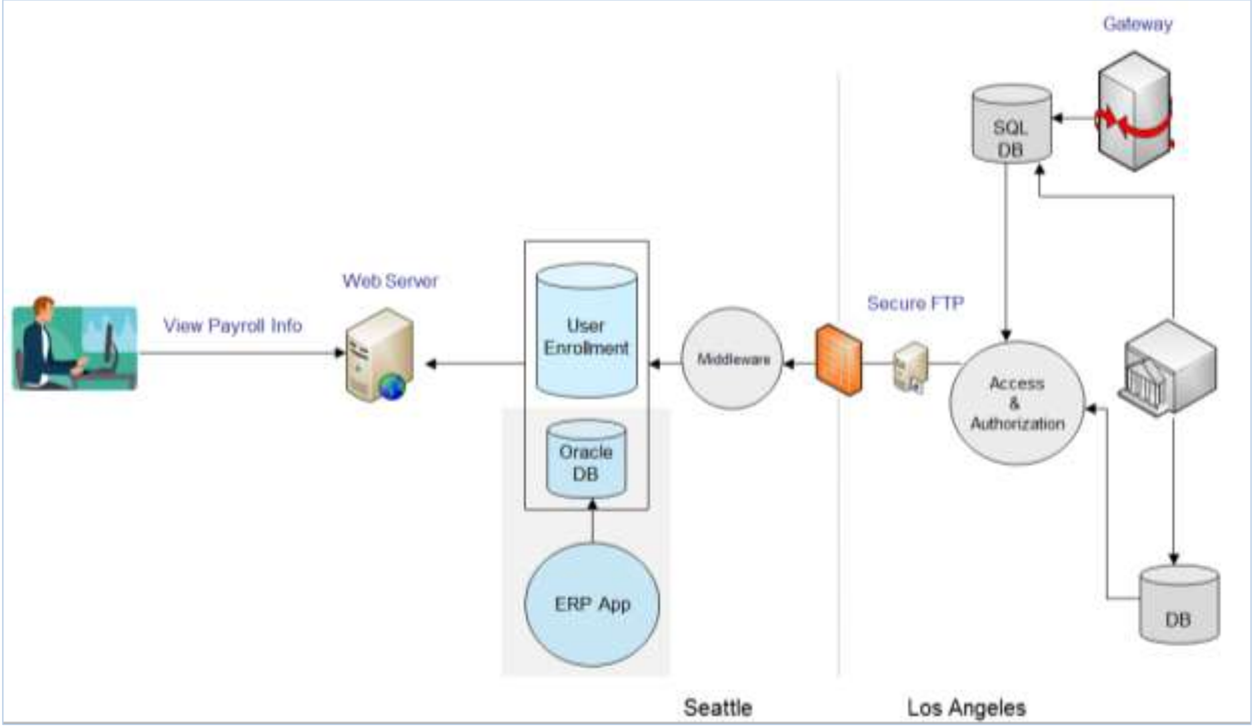


Figure 3-18. Example of Storage Array Illustration

3.10.5 Addressing the Data Flow Diagram (§ 10.1.4 in SSP)

Section 10.1.4 in the System Security Plan template requires that you include a data flow diagram of how network traffic flows through your platform and offering. A data flow diagram focuses more on the direction of the network traffic and less on the actual network topology. However, certain components of the system's network topology need to be included in order to illustrate the direction that the network traffic flows through the system. Figure 3-19 below shows an example of a data flow diagram.



Source: FISMA Center

Figure 3-19. Data Flow Diagram Example

3.11 DESCRIBING THE SECURITY CONTROLS IN THE SSP (§ 13 IN SSP)

Section 13 in the *System Security Plan* template requires that CSPs accurately describe how security controls are implemented. Your information system and offering likely includes multiple components. When describing a security control, you will need to describe how the control is implemented for all components of your system as is illustrated in Figure 3-20. It may be possible that different services provided by a vendor consist of different components. Some components may be common across all services but others may be unique to a particular service.

You may describe how a control is implemented based on its named component (Figure 3-5), or its functional component name (Figure 3-6). It adds clarity to the control description process if the functional components are aligned with named components however that may not be possible in all cases.

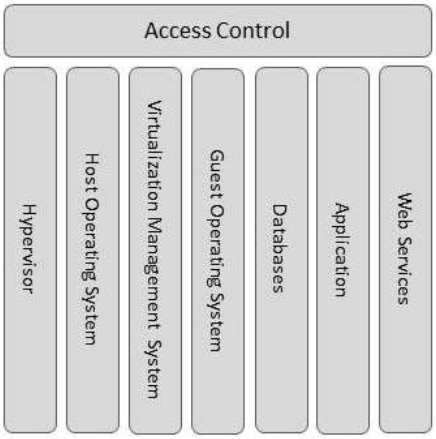


Figure 3-20. Access Control for System Components

Tip: If all components are integrated into a centralized single sign-on system, then the access control process and implementation only needs to be described once.

FedRAMP allows for flexible implementations, and it is possible that a group of components collectively use one type of access control mechanism and that the rest of the components use a different access control mechanisms as illustrated in Figure 3-21.

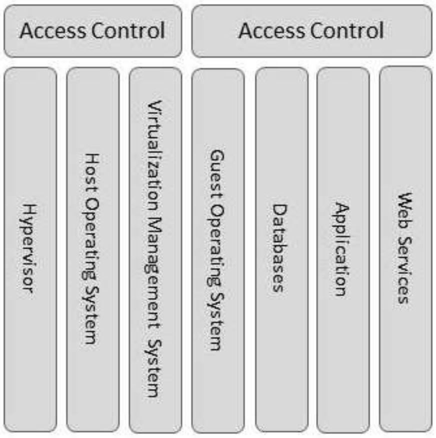


Figure 3-21. Two Access Control Mechanisms

If multiple access control mechanisms are used for the various system components, when describing how access controls are implemented, CSPs need to describe all access control mechanisms and indicate which components use which mechanism.

3.11.1 Security Control Summary Information

Each security control includes a table called Security Control Summary Information as illustrated in Table 3-3. Security control enhancements also require security control summary information. Definitions for Control Origination can be found in Table 3-4. For any of the "-1" controls that describe Policies and Procedures (e.g. AC-1, SC-1 etc.) it is not possible to select Configured by Customer, Provided by Customer, Shared, or Inherited from pre-existing Provisional Authorization and this is by design since all organizations need to have their own set of Policies and Procedures.

Table 3-3. Example of Security Control Summary Information

Control ID	Control Summary Information
Responsible Role:	
Parameter:	
Implementation Status (check all that apply): □ In place □ Partially implemented □ Planned □ Alternative implementation □ Not applicable	
Control Origination (check all that apply): □ Service Provider Corporate □ Service Provider System Specific □ Service Provider Hybrid (Corporate and System Specific) □ Configured by Customer (Customer System Specific) □ Provided by Customer (Customer System Specific) □ Shared (Service Provider and Customer Responsibility) □ Inherited from pre-existing Provisional Authorization (PA) for <**Information System Name**>, <**Date of PA**>	

In the field described as Responsible Role, the CSP should indicate what staff role within their organization is responsible for maintaining and implementing that particular security control. Examples of the types of role names may differ from CSP to CSP but could include role names such as:

- System Administrator
- Database Administrator
- Network Operations Analyst
- Network Engineer
- Configuration Management Team Lead
- IT Director

- Firewall Engineer

All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement and manage the control. In some cases, the responsibility is shared by a CSP and by the customer. Since each service offering is unique, the FedRAMP program cannot provide guidance on which controls should or should not be defined according to the Control Origination definitions in Table 3-4.

Table 3-4. Control Origination Definitions

Control Origination	Definition	Example
Service Provider Corporate	A control that originates from the CSP corporate network.	DNS from the corporate network provides address resolution services for the information system and the service offering.
Service Provider System Specific	A control specific to a particular system at the CSP and the control is not part of the standard corporate controls.	A unique host based intrusion detection system (HIDs) is available on the service offering platform but is not available on the corporate network.
Service Provider Hybrid	A control that makes use of both corporate controls and additional controls specific to a particular system at the CSP.	There are scans of the corporate network infrastructure. Scans of databases and web based application are system specific.
Configured by Customer	A control where the customer needs to apply a configuration in order to meet the control requirement.	User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http or https, etc.), entering an IP range specific to their organization are configurable by the customer.
Provided by Customer	A control where the customer needs to provide additional hardware or software in order to meet the control requirement.	The customer provides a SAML SSO solution, adding in SAML assertions, to implement two-factor authentication.
Shared	A control that is managed and implemented partially by the CSP and partially by the customer.	Both the service provider and the customer require two-factor authentication for both privileged and non-privileged users for network access.

As of this edition, guidance has been provided for a subset of the security controls. This document may be updated in the future to include guidance on other security controls.

3.11.2 Security Control AC-7

Section 13.1.7(a) in the *System Security Plan* template requires that you discuss the fact that unsuccessful logins are set to a parameter of 3 or less within a 15 minute period.

Questions that you should consider in your discussion are:

- Is the unsuccessful login parameter configured on a central policy server? What server?
- Is the unsuccessful login parameter configured manually on a server by server basis?
- What tool/function do you use to configure unsuccessful logins?
- Do you use policy templates or a policy manager to configure this parameter?
- Is the unsuccessful login parameter configured the same for all groups and roles of users?
- Is the unsuccessful login parameter configured using different techniques on application servers, databases, firewalls, routers, and all other components?
- Do you use a single sign-on application that controls unsuccessful login parameters?
- Do you configure unsuccessful login parameters through a GUI or a CLI?
- Do you use any COTS authentication/access control products to configure the unsuccessful login parameter?
- Can you provide any screenshots that show the configuration of the unsuccessful login parameter is configured?
- If you are using multiple operating systems do you set this parameter using different techniques for the different operating systems?

Section 13.1.7(b) in the *System Security Plan* template requires that you discuss how account lockouts occur when a user has more than 3 unsuccessful login attempts within a 15 minute period.

Questions that you should consider in your discussion include:

- Are account lockouts configured on all systems that are within the boundary?
- Are account lockouts configured on any customer control panel login mechanisms?
- If a user is locked out, how will they know who to call to have their account reset?
- Will VPNs made available to customers through self-service control panel's lockout via the physical system lockout parameters? Or do customers need to configure their own VPN lockouts separately?

3.11.3 Security Control IA-5(3)

Section 13.7.5.1.3 in the *System Security Plan* template requires that you discuss how HSPD12 card registrations are performed in person. If you use smart cards for two-factor authentication, they must be HSPD12 and registration must take place in person. This control does not mean that using HSPD12 cards is a requirement for two-factor authentication. If your system does not use HSPD12 cards, this control is not applicable to your system and is not implemented.

3.11.4 Security Control PE-2(a)(b)(c)

Section 13.11.2 in the *System Security Plan* template requires that you discuss how physical access authorizations are implemented.

Questions that you should consider in your discussion include:

- Is there a list of who has access to the data center?
- Who authorizes access to data center?
- Are there different authorization levels for different physical areas? (e.g. chillers, electrical substation room, UPS/battery room, generator area)
- Are there different types of authorization credentials? If yes, what are they?
- Are the data center access list and authorization credentials reviewed at least once annually?

3.11.5 Security Control PE-3(a)(b)(c)(d)(e)(f)(g)

Section 13.11.3 in the *System Security Plan* template requires that you discuss how physical access authorizations are enforced?

Questions that you should consider in your discussion include:

- What is used to control access to the data center? (e.g. hand scanner, card key)
- Are there separate access control devices for the electrical substation room, battery room, chillers, generators?
- What is the make/model of the access control devices?
- If PINs or passwords are used, do they meet the password change requirement frequency?
- How does the access control device verify an individual's identity?
- Are cages/racks locked?
- Are there guards at the data center entrance?
- Are areas considered publicly accessible areas controlled?
- On what date were physical access control devices were last inventoried?
- On what date were keys and combination locks last changed?

3.11.6 Security Control PE-4

Section 13.11.4 in the *System Security Plan* template requires that you discuss how access control for transmission medium is implemented.

Questions that you should consider in your discussion include:

- Do wiring closets and patch panels have locks? Who has access?
- Are there exposed telecomm jacks that are not locked?

- Where does telecomm circuit/Internet connectivity enter the data center?
- Are cables and wires below the floor?
- Are cables and wires in inaccessible (locked) ceiling trays?

3.11.7 Security Control PE-5

Section 13.11.5 in the *System Security Plan* template requires that you discuss how access control to display mediums is implemented.

Questions that you should consider in your discussion include:

- Are there printers or monitors located in open access areas in the data center?
- Are printers/monitors in the data center password protected?
- Are surveillance cameras pointing at printers and monitors?
- What systems print to printers located in the data center?
- Who can access monitors, printers, fax machines and other output devices in the data center and who authorizes their access?

3.11.8 Security Control PE-6(a)(b)(c)

Section 13.11.6 in the *System Security Plan* template requires that you discuss how monitoriong of physical access is implemented.

Questions that you should consider in your discussion include:

- Are guards located at data center entrances? Are they armed?
- Are balusters outside the data center building near entrance areas?
- Are cameras pointed at data center entrances? What kind of cameras are being used?
- If cameras are being used, how long is recorded media kept for?
- Are hand scanners used to at data center entrances? What make and model are they?
- Are access logs to hand scanners reviewed? If yes, who reviews them?
- Are sign in sheets required at data center entrances? Who reviews these sheets?
- Are card keys required at data center entrances?
- Are access logs to card keys reviewed? If yes, who reviews them?

3.11.9 Security Control PE-6(1)

Section 13.11.6.1.1 in the *System Security Plan* template requires that you discuss how monitoriong of real-time physical intrusion alarms and surveillance equipment is monitored.

Questions that you should consider in your discussion include:

- Is there an alarm system installed at the data center?
- What events will set off the alarm system?

- Does an outside service provider maintain and manage the alarm system?
- When was the alarm system last tested or inspected?
- Are cameras located inside the data center?
- Does an outside service provider maintain and manage the surveillance cameras?
- When were the cameras last tested or inspected?

3.11.10 Security Control PE-13 (1)(2)(3)

Section 13.11.13 in the System Security Plan template requires that you describe fire suppression security controls. One of the things that you should indicate is whether or not your fire suppression system complies with NFPA 75[1]. Indicate if local fire marshals have performed a recent inspection and what the date is of the last inspection.

Questions that you should consider in your discussion are:

- Is there a fire alarm system?
- Do fire alarms get sent to a remote monitoring center?
- How are your alarms activated? (e.g. smoke, heat)
- Where are fire detection devices located?
- Where are fire suppression devices located?
- Is the monitoring and maintenance of the system outsourced to a service provider?
- Are there maintenance records for the fire suppression system?
- Are you using wet pipe, dry pipe, pre-action, or deluge sprinklers?
- Are you using an inert agent fire suppression system?
- Are there fire extinguishers in the data center?
- Where are fire extinguishers located?
- When are fire extinguishers inspected?
- What fire suppression agent do the fire extinguishers use?

3.11.11 Security Control PL (4)

Section 13.12.3 in the *System Security Plan* template requires that CSPs provide Rules of Behavior for their users. FedRAMP has provided a template for Rules of Behavior which is available on the FedRAMP website. The template includes two sample sets of Rules of Behavior – one for Internal Users and one for External Users.

Internal Users are company employees or company contractors.

External Users are customers who will be using the service provider platform.

Before the CSP gives customers access to the service provider platform, CSPs should require

[1] National Fire Protection Association (NFPA) Standard for the Protection of Information Technology Equipment 75

their customers to sign the External Rules of Behavior. If the CSP provisions one account to one customer user (a customer account administrator), who in turn provisions accounts for the all the other customer users, the CSP only needs to obtain a signed External Rules of Behavior for that one customer user. That one customer user who provisions accounts for other customer users inside their respective agency will then become responsible for ensuring that Rules of Behavior for their agency are signed for the system. The agency customer account administrator should then determine the appropriate Rules of Behavior for the agency users to sign – but should take into consideration the rules listed on External Rules of Behavior that was signed and provided to the CSP.

The general rule of thumb is that if you provision an account to someone else, the person who provisions the account is responsible for obtaining a signed Rules of Behavior. In some cases the person provisioning the account might be the CSP, and in some cases the person provisioning the account might be an agency employee.

The rules provided on the FedRAMP Template are samples and CSPs do not have to use these specific rules. CSPs should consider what rules apply to the candidate system and edit the template to describe the rules that are actually required. They can use any of the sample rules, or replace them completely with other rules. Signed records of the Rules of Behavior should be retained by the entity that provisions the account. It is acceptable to implement the Rules of Behavior electronically or on paper, however, agreement to the Rules of Behavior and sign-off should be obtained before users are granted access to new accounts.

3.11.12 Security Control SA-11(1)

Section 13.15.11.1.1 in the *System Security Plan* template is a control for original source code development. If the CSP service offering has been developed using original source code, CSPs need to provide a code analysis report that shows that the latest release was scanned with a code analysis scanner. Indicate what scanner was used and insert the report into your *System Security Plan* for this control. All code analysis reports should be made available to the 3PAO that performs the testing on the CSP system. If the CSP is not writing any original code, then this control is not applicable and that should be indicated in the *System Security Plan*.

3.11.13 Security Control SC-7 (1)

Section 13.16.6.1.1 in the *System Security Plan* template and SC-7(1) references the Trusted Internet Connection (TIC) initiative. The TIC initiative is mandated by OMB in Memo M-08-05[2]. The purpose of putting in place Trusted Internet Connections (TIC) is to reduce and consolidate and connections to the federal government, including connections to the Internet. Additionally, data must pass through the TIC to obtain monitoring services from US-CERT.

Currently, there are two categories of TICs as defined and approved by Federal Network Services

[2] http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf

which is part of the Department of Homeland Security (DHS):

- Federal agencies that are approved TIC Access Providers (referred to as TICAPs)
- Networx Managed Trusted IP Service providers with qualified and approved capabilities (referred to as MTIPS).

For a commercial cloud service provider to comply with SC(7)-1, the CSP must demonstrate an architecture that allows an agency to provide effective separation of network traffic to meet the following objectives:

a. All government data, shall be capable of routing through a dedicated logical or physical network connection.

b. The service shall be capable of excluding co-tenant data, or any other third party data, not intended for the government from being transmitted through a government network connection.

c. The service shall be capable of excluding data intended solely for government use from being routed through an external (non-dedicated) network connection.

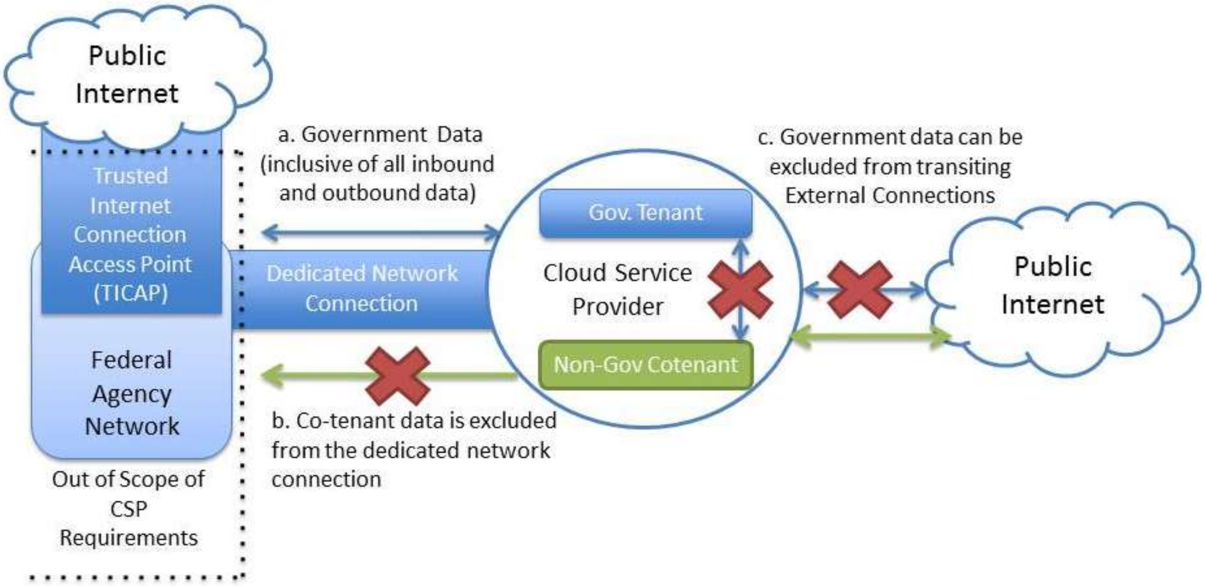

Public Internet
Trusted Internet Connection Access Point (TICAP)
Federal Agency Network
Out of Scope of CSP Requirements
a. Government Data (inclusive of all inbound and outbound data)
Dedicated Network Connection
b. Co-tenant data is excluded from the dedicated network connection
Gov. Tenant
Cloud Service Provider
Non-Gov Cotenant
c. Government data can be excluded from transiting External Connections
Public Internet

Figure 3-22. TIC Compliant Architecture

To accomplish the TIC objectives, there are multiple architectures that CSPs may propose with an example illustrated in Figure 3-22. The following architectures have been previously approved by Federal Network Services:

1. CSP routes all Government traffic via VPN back to an agency network.

2. CSP routes all government traffic through an agency sponsored MTIPS, no government traffic is allowed over the public Internet.

3. CSP routes all government traffic through dedicated network connections to an agency network, no government traffic is allowed over the public Internet.

4. CSP routes by all government traffic through government endpoints, not allowing any data to traverse any other end-points than agency IP address ranges (effectively all inbound/outbound traffic routes through government network by proxy or other rules).

It is not possible for a CSP to connect directly to a TICAP. Connection to an MTIPS Provider is available through the Networx contract but this contract vehicle can only be used by agencies. Agencies should sponsor the CSP that they want to use, and then use the Networx contract vehicle to assist the CSP in connecting to the MTIPS Provider. More information about the Networx contract can be found at the following URL: http://www.gsa.gov/portal/content/104870 .

More information on the TIC is available at the following URL: http://www.dhs.gov/files/programs/gc_1268754123028.shtm . The TIC Program Office can be contacted at dhs@tic.gov.

3.11.14 Security Control SC-13

Section 13.16.12 in the *System Security Plan* template and SC-13 requires that you discuss where cryptographic protections are implemented. Cryptographic protections can be used in a multitude of places on an information system. You should describe what components or devices use cryptographic protections and how they are implemented.

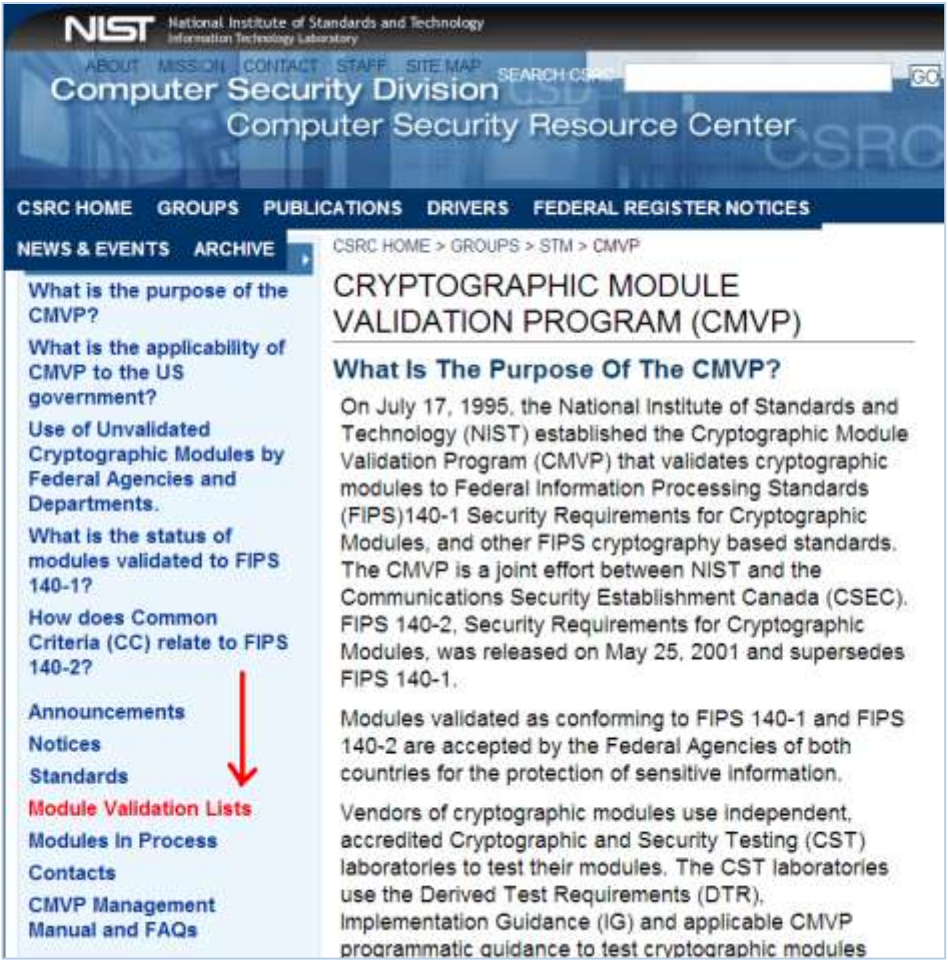
Questions that you should consider in your discussion are:

- Are data partitions encrypted?
- Are swap partitions encrypted?
- Are temporary file systems encrypted?
- Are file systems encrypted?
- Are files encrypted? All files or just some files?
- Are storage devices encrypted?
- Are log files encrypted?
- Are databases encrypted?
- Are hardware encryption modules used?
- Are encrypted logical volumes used?
- Do virtual machines that are not running have their images/templates encrypted?
- Are commercial off-the-shelf encryption products being used? Which ones?

If cryptographic protections are used to protect data in transmission, save that discussion for Section 13.16.8 in the *System Security Plan* which is where you describe the control implementation for Transmission Confidentiality SC-9.

3.11.15 Security Control SC-13(1)

Section 13.16.12.1.1 in the *System Security Plan* template and SC-13(1) requires that you employ FIPS 140-2 cryptography to protect unclassified information. You can find out if the products that use cryptography on your system have been FIPS 140-2 validated by looking for a validation certificate for that product on the Cryptographic Module Validation Program (CMVP) website. Click on *Module Validation Lists* as shown in Figure 3-23 to search for products used by your system.


NIST National Institute of Standards and Technology
Information Technology Laboratory
ABOUT
MISSION
CONTACT
STAFF
SITE MAP
SEARCH CSRC
GO
Computer Security Division
Computer Security Resource Center
CSRC
CSRC HOME
GROUPS
PUBLICATIONS
DRIVERS
FEDERAL REGISTER NOTICES
NEWS & EVENTS
ARCHIVE
CSRC HOME > GROUPS > STM > CMVP
What is the purpose of the CMVP?
What is the applicability of CMVP to the US government?
Use of Unvalidated Cryptographic Modules by Federal Agencies and Departments.
What is the status of modules validated to FIPS 140-1?
How does Common Criteria (CC) relate to FIPS 140-2?
Announcements
Notices
Standards
Module Validation Lists
Modules In Process
Contacts
CMVP Management Manual and FAQs

CRYPTOGRAPHIC MODULE VALIDATION PROGRAM (CMVP)

What Is The Purpose Of The CMVP?

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS)140-1 Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC). FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 and supersedes FIPS 140-1.

Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

Vendors of cryptographic modules use independent, accredited Cryptographic and Security Testing (CST) laboratories to test their modules. The CST laboratories use the Derived Test Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules

Figure 3-23. Module Validation Lists

Validation certifications always apply to a specific product version number. If you patch a product, the patch disqualifies the FIPS 140-2 validation (even if it makes the product more secure). If the patch is non-security related, CMVP IG G.8 defines a path for a validation update that is timely and cost effective (1SUB). CMVP IG G.8 also addresses how such changes can be re-validated. Please refer to the FIPS 140-2 Standards for more information.

Note: FIPS 140-2 Standards can be found at the following URL:
http://csrc.nist.gov/groups/STM/cmvp/standards.html#02

In some hardware appliances that use a Hardware Security Module (HSM), where the encryption is performed entirely on the HSM, the validation certificate is listed in the name of the HSM vendor, and not in the name of the appliance vendor.

Once you have located the validation certificate, you can provide the certificate information in your *System Security Plan* by:

- Putting in a URL to the certificate
- Taking a screenshot of the certificate and pasting it in your plan
- Downloading the certificate (.pdf file) and including it with your *System Security Plan*.

3.12 SECURITY ALERTS & ADVISORIES (SI-5)

Section 15.7.5 in the System Security Plan requires that you discuss how you receive information system security alerts, advisories, and directives from designated external organizations. One of these external organizations should be US-CERT. A recommendation is that you receive advisories from all vendors you are using (e.g. operating system vendors, database vendors, router vendors etc.).

It is often easiest to send all advisories to one internal list such as advisories@cspname.com or security@cspname.com. You can then add staff members to those distribution lists as needed. Keep in mind that this control needs to be auditable. Therefore, you need to be able to show that advisories are in fact coming in to your company and you need to be able to provide a list of who is receiving these advisories.

3.13 IT CONTINGENCY PLAN (CP-2)

FedRAMP provides an *IT Contingency Plan (ITCP)* template that is available on the FedRAMP website. Please refer to NIST SP 800-34, Revision 1 for assistance in writing your IT Contingency Plan http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.

3.14 BUSINESS IMPACT ANALYSIS (BIA)

The *Business Impact Analysis* is an Appendix of the *IT Contingency Plan*. At this time, FedRAMP does not provide a template for the BIA. Please refer to NIST SP 800-34, Revision 1 for more information on developing a *Business Impact Analysis*.

3.15 CONFIGURATION MANAGEMENT PLAN (CM-9)

The FedRAMP program currently does not provide a template for a *Configuration Management*

Plan. However, each CSP is required to submit a *Configuration Management Plan* which should describe how their organization controls change for the information system. The *Configuration Management Pla*n needs to be able to stand alone since it is possible that the staff that uses the *Configuration Management Plan* does not have access to the *System Security Plan*. The *Configuration Management Plan* need to address the Configuration Management (CM) family of security controls as indicated in the *System Security Plan* template. A summary of the CM controls can be found in the Table 3-5.

Table 3-5. Configuration Management Controls

Control No	Control Name	Low	Moderate	Delta From NIST 800-53 r3
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	No
CM-2	Baseline Configuration	CM-2	CM-2 (1) (3) (4)	Yes
CM-3	Configuration Change Control	Not Selected	CM-3 (2)	Yes
CM-4	Security Impact Analysis	CM-4	CM-4	No
CM-5	Access Restrictions for Change	Not Selected	CM-5	No
CM-6	Configuration Settings	CM-6	CM-6 (3)	Yes
CM-7	Least Functionality	CM-7	CM-7 (1)	Yes
CM-8	Information System Component Inventory	CM-8	CM-8 (1) (5)	Yes
CM-9	Configuration Management Plan	Not Selected	CM-9	No

Configuration management nomenclature should be defined in the *Configuration Management Plan* as it is used at the CSP. Suggested configuration management nomenclature that is worth taking into consideration can be found in Table 3-6. FedRAMP allows for flexibility of development and release nomenclature and the definitions in Table 3-6 may not match the terminology that your organization is accustomed to using. Please modify the definitions in Table 3-6 to match the nomenclature that you normally use. If you don't normally use the terminology found in Table 3-6, but would like to switch to this terminology, please ensure that all of your supporting documents are updated so that the terminology is consistent across all of your documentation.

Table 3-6. Configuration Management Nomenclature

Nomenclature	Definition
Alpha Release	The Alpha phase of the release cycle is the first phase to begin software testing. Alpha releases can potentially contain stability issues and are not made available to customers.
Beta Release	The Beta phase of the release cycle is a secondary phase to begin software testing after all features of the code are complete and after bugs found during the Alpha Release have been fixed.

Nomenclature	Definition
Baseline	(1) A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures. (2) A document or a set of such documents formally designated and fixed at a specific time during the life cycle of a configuration item. (3) Any agreement or result designated and fixed at a given time, from which changes require justification and approval. (IEEE Std. 610-12-1990). A baseline is configuration identification formally designated and applicable at a specific point in the life cycle of a configuration item.
Build	An operational version of a system or component that incorporates a specified subset of the capabilities that the final product will provide. (IEEE Std. 610-12-1990)
Configuration (or Change) Control Board (CCB)	A group of people responsible for evaluating and approving or disapproving proposed changes to configuration items, and for ensuring implementation of approved changes. (IEEE Std. 610-12-1990)
Change Request	A request from either an internal or an external customer to make a change to a baseline configuration. Change requests can be related to either software releases or to network components such as server or workstation configurations or to any other network infrastructure component.
Configuration Control	An element of CM, consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification. (IEEE Std. 610-12-1990)
Configuration Item	An identifiable part of a system that is a discrete target of configuration control processes. (NIST SP 800-128)
Configuration Management	A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements. (IEEE Std. 610-12-1990)
Release	A software build that has been thoroughly tested and made available to customers.
Hardware Baseline	A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support <Information System Name> operations is maintained by the Configuration Control Board (CCB) and is part of the Hardware and Software Inventory. A backup copy of the inventory is stored in a fire-rated container located or otherwise not collocated with the original.
Software Baseline	A current and comprehensive baseline inventory of all software that includes manufacturer, type, and version and installation manuals and procedures. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.

Nomenclature	Definition
Version	Each software build is assigned a version number. The version number is used as a mechanism for differentiating one build from another. Version numbers are used regardless of whether or not a build is ultimately released.

Note: NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems* can be found at the following URL: http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf

When there is a major change to your system, you are required to update certain artifacts and new security testing may be required on all of your controls or a subset of your controls. If you have a major change to your system planned, please notify your FedRAMP ISSO in advance of the change giving as much advanced notice as possible. The nomenclature such as that found in Table 4-3 should be taken into consideration when you implement a major change to your system.

Within your Configuration Management Plan, you are required to describe the change management process that you use to implement changes (CM-3). Your change management process should indicate if the change is a major change, a standard change, or an emergency change (CM-3a). You are welcome to add other change types according to your organizational needs.

A major change includes (but is not limited to):

- Changing your authentication or access control implementation
- Changing your storage implementation
- Implementing a new code release of your code
- Changing your backup mechanisms and process
- Changing your IaaS provider (if you are a PaaS or SaaS provider)
- Adding new interconnections to outside service providers
- Changing an alternate (or compensating) control
- Removing security controls
- An addition or change to functionality or services
- A change in the system boundary definition (e.g. adding new data center
- A change to the account provisioning process

The following types of changes should always be handled through your standard Configuration Management change control process:

- Changing a COTS product implemented in your system to another vendor or product
- Changing a product that delivers like functionality (e.g. a scanner, a firewall)
- Any change related to patch management
- A configuration change

- Adding or changing a firewall rule or a router ACL
- Emergency change

3.16 INCIDENT RESPONSE PLAN (IR-8)

Security 13.8.8 in the *System Security Plan* template requires that you develop an *Incident Response Plan*. FedRAMP currently does not provide a template for an *Incident Response Plan*. Nonetheless, each CSP is required to submit an *Incident Response Plan* which should describe how they manage security incidents for the system. The Incident Response Plan needs to address the Incident Response (IR) family of security controls as indicated in the *System Security Plan* template. A summary of the IR controls is found in Table 3-7. The *Incident Response Plan* (IR-8) for the system should include information that provides descriptions of how IR-1 through IR-7 are implemented.

Table 3-7. Incident Response Controls

Control No	Control Name	Low	Moderate	Delta From NIST 800-53 r3
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	No
IR-2	Incident Response Training	IR-2	IR-2	No
IR-3	Incident Response Testing & Exercises	Not Selected	IR-3	Yes
IR-4	Incident Handling	IR-4	IR-4 (1)	Yes
IR-5	Incident Monitoring	IR-5	IR-5	No
IR-6	Incident Reporting	IR-6	IR-6 (1)	No
IR-7	Incident Response Assistance	IR-7	IR-7 (1) (2)	Yes
IR-8	Incident Response Plan	IR-8	IR-8	Yes

The purpose of the *Incident Response Plan* is to have a plan to use in the event of a security or privacy incident, or any other incident that may affect operations of the system (e.g. incidents related to power outages, natural disasters). The staff that may need to use the *Incident Response Plan* may not have access to the *System Security Plan*. Therefore, the *Incident Response Plan* should be able to stand alone. It is important to make sure that incident response roles and responsibilities are well defined and articulated in the *Incident Response Plan*.

Questions that you should consider in your discussion on IR-8, part (a) include:

- Are incident roles and responsibilities defined?
- Who is responsible for incident response planning?
- Are there clear lines of reporting related to incidents?
- Are incident types defined?
- When was the *Incident Response Plan* last reviewed and who approved it?
- How does incident response fit into the overall Information Security Program?

- Do you track how many incidents occur each month/year?
- Do you track what types of incidents are most prevalent?
- Do you track the average time it takes to close an incident?

Questions that you should consider in your discussion on IR-8, part (b) include:

- To whom has the *Incident Response Plan* been distributed to in your organization?
- Does the *Incident Response Plan* indicate that designated FedRAMP personnel should be included in the distribution?

Questions that you should consider in your discussion on IR-8, part (c) include:

- How often is the *Incident Response Plan* reviewed?
- When was the *Incident Response Plan* last reviewed?

Questions that you should consider in your discussion on IR-8, part (d) include:

- Does the Incident Response Plan include a document history to record changes?
- Who is responsible for updating the plan with revisions?
- Were any revisions made after the last testing exercise?

Questions that you should consider in your discussion on IR-8, part (e) include:

- If there is a change to incident response procedures or policies who is notified?
- Is there an organizational contact list included for the incident response team members?
- Are role names listed for the individuals identified in the contact list?

Additional FedRAMP requirements for IR-8(b) and IR-8(e) require that you include FedRAMP points of contact in your incident response plan. Please obtain FedRAMP points of contact from your designated FedRAMP ISSO.

When you contract with customer agencies to use your cloud service platform, you will need to obtain points of contact from each customer agency on who to notify at the agency in the event of a security incident. Please insert a copy of Table 3-8 into your *Incident Response Plan* and fill it out as you contract with new customers. One of the points of contact should be the agency CSIRC[3]. You should list the points of contact in the order in which the agency has specified. Your *Incident Response Plan* is required to be updated no less than once annually. At the time of the annual update, you should contact your customer agency and make sure that each of the phone numbers and POCs listed are still accurate.

3.11.16 Security Control IR-2

Section 13.8.2 in the *System Security Plan* requires that you describe how personnel are trained

[3] Computer Security Incident Response Center

in incident response for the system.

Question that you should consider in your discussion include:

- What roles are trained? (e.g. database administrator, systems administrator)
- On what date did the last training occur?
- When will the next training take place?
- Where did the training take place and was it online or in person?
- Is there a participant/attendance list of who participated in the last training?
- Who is responsible for ensuring the training takes place?

3.11.17 Security Control IR-3

Section 13.8.3 in the *System Security Plan* requires that you perform an annual incident response test/exercise.

Questions that you should consider in your discussion include:

- What roles participate in the incident response test/exercise?
- On what date did the last test/exercise occur?
- When will the next test/exercise occur?
- Where did the test/exercise occur?
- Is there a participant list of who participated in the last text/exercise?
- Who is responsible for leading the test exercise?
- Who is responsible for writing the test plan that must be submitted to FedRAMP annually?

3.11.18 Security Control IR-4

Section 13.8.6.5 in the *System Security Plan* requires that you describe your incident handling capability.

Questions that you should consider for part (a) include:

- How do you prepare for incidents?
- Who should agency customers call if they suspect an incident?
- Is there an incident hotline or phone number published where customers can see it?
- What capability do you have to detect incidents?
- If you suspect an incident how do you verify if it really is an incident?
- What methods do you use to analyze confirmed incidents?
- What methods do you use to contain incidents?
- What methods do you use to eradicate incidents?
- What is your process for determining that the system has recovered from the incident?

Questions that you should consider for part (b) include:

- Which incident handling activities are coordinated with contingency planning activities?
- How does the coordination take place?
- Which incident handling activities are coordinated with contingency planning activities?

Questions that you should consider for part (c) include:

- Who maintains archives of lessons learned regarding incidents?
- How do you determine which incidents require a lessons learned report?
- How soon after an incident is closed will the lessons learned report be published?
- Who is responsible for integrating lessons learned into procedures, training, and test/exercises?

Questions that you should consider in your discussion for the additional FedRAMP requirements and guidance for IR-4 include:

- What personnel security requirements are required of individuals who perform incident handling?

3.11.19 Security Control IR-4(1)

Section 13.8.4.1.1 in the *System Security Plan* template requires that you describe the automated mechanisms for incident handling?

Questions that you should consider in your discussion include:

- Is there any sort of online workflow tool used for managing incidents?
- Are there any automated alerts related to incidents?
- Are there any automated programs, scripts, or applications that look for incidents or suspicious activities?

3.11.20 Security Control IR-5

Section 13.8.5 in the *System Security Plan* template requires that you describe how security incidents are tracked and documented.

Questions that you should consider in your discussion include:

- What mechanism is used to record and track information about incidents?
- Do you have an incident reporting and tracking form?
- Is the incident reporting form online on your intranet? Where?
- Is the incident reporting form a .pdf file?
- Can you insert a blank copy of the incident reporting form?

- Is there a place on the incident reporting form to indicate if PII[4] has been compromised?
- Who is responsible for ensuring that incidents are documented internally?
- Who will be the FedRAMP point of contact for incidents?
- Who will be the point of contact for customer agencies
- Is there a flow chart to show how decisions about incident escalation are made?

3.11.21 Security Control IR-6

Section 13.8.6 in the *System Security Plan* template requires that you describe incident reporting capabilities.

Questions you should consider in your discussion for part (a) include:

- What notification timeframes are built into your incident reporting process?
- Do your reporting timeframes line up with Table J-1 in NIST SP 800-61, Revision 1?

Questions that you should consider in your discussion for part (b) include:

- Who will ensure that incident reporting timeframes are adhered to?
- Who at your company determines if law enforcement should be notified?
- What decisions need to be made before law enforcement is notified?
- Do you have the contact information for all of your agency customers?

Additionally, see Section 3.12 in this document for more information on incident reporting part (b).

Table 3-8 should be inserted in the section related to incident reporting (IR-6). As CSPs contract with new customers, agency contact information should be recorded in this table. In the event of a security incident, the CSP should contact all agency customers using their system as well as the FedRAMP ISSO.

Table 3-8. Agency Points of Contact to Report Incidents

Agency Name	Point of Contact	Phone	Email
<Agency Name>	1.	1. Primary: 2. Alternate:	
	2.	1. Primary: 2. Alternate:	
	3. CSIRC		
<Agency Name>	1.	1. Primary: 2. Alternate:	

[4] Personally Identifiable Information

Agency Name	Point of Contact	Phone	Email
	2.	1.Primary: 2. Alternate:	
	3. CSIRC		

3.11.22 Security Control IR-6(1)

Section 13.8.6.1.1 in the *System Security Plan* template requires that you describe automated mechanisms to assist in the reporting of security incidents.

Questions that you should consider in your discussion include:

- Is there an online Incident Reporting Form that is available to your staff?
- Is there an online Incident Reporting Form that is available to your customers?
- Are there any apps for Incident Reporting?

3.11.23 Security Control IR-7

Section 13.8.7 in the *System Security Plan* template requires that you provide incident response assistance and resources for users.

Questions that you should consider in your discussion include:

- Have you identified incident response experts within your own organization?
- Do you have an internal Intranet page or wiki that includes helpful information for users about security incidents and reporting?

3.11.24 Security Control IR-7(1)

Section 13.8.7.1.1 in the *System Security Plan* template requires that you provide mechanisms to increase the availability of incident response related information and support.

Questions that you should consider in your discussion include:

- Is there an incident reporting phone number that is available 24 x 7 x 365?
- Is there an internal web page or wiki with incident reporting information that has high-availability mechanisms built into it?
- Do you have contact information for at least one outside vendor that specializes in incident response?
- Do you have any contracts with outside vendors to provide incident response?

3.11.25 Security Control IR-7(2)

Section 13.8.7.1.2 in the *System Security Plan* template requires that you describe incident response capabilities that extend beyond your own organization.

Part (a) requires that you establish a direct, cooperative relationship between your incident response capabilities and external providers of information system protection.

Questions that you should consider in your discussion for part (a) include:

- Have you documented the process on how to contact your vendors if you suspect a security vulnerability in a COTS product?
- Does your organization receive patch update information from all of your different vendors? Who receives information on the latest patches?
- Does your organization receive advisories from US-CERT? Who receives the advisories?

Part (b) requires that you provide your internal incident contact information to external providers.

Questions that you should consider in your discussion for part (b) include:

- What are the incident points of contact available to agency customers?
- Do your Internet providers have your internal points of contact for incidents?
- Do your telecom providers have your internal points of contact for incidents?
- If you use an external IaaS or PaaS vendor, does that vendor have your internal incident response POCs?

3.17 POA&M TEMPLATE

CSPs should leverage the *Security Assessment Report* to put together a *Plan of Action & Milestones* (POA&M) for mitigating security weaknesses. FedRAMP provides a POA&M template for CSPs which is available on the FedRAMP website. All High and Moderate findings from the *Security Assessment Re*port should be mapped into the POA&M. High impact vulnerabilities need to be mitigated within 30 days, and Moderate impact vulnerabilities need to be mitigated within 90 days.

4. INSTRUCTIONS FOR CSPS ON MAINTAINING THE AUTHORIZATION

4.1 ONGOING ASSESSMENT AND CONTINUOUS MONITORING

OMB Circular A-130 Appendix III requires that security controls in information systems be reviewed at least every three years or when there are significant modifications to the system. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system.

Note: You can find OMB Circular A-130 Appendix III at the following URL: http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii

The FedRAMP program provides a *Continuous Monitoring Strategy & Guide* to provide instructions on the continuous monitoring process. Please refer to that guide for more information on continuous monitoring.

5. GENERAL DOCUMENTATION INFORMATION FOR CSP

5.1 FORMATTING AND SECTION NUMBERS

The templates that are provided by the FedRAMP program are provided to simplify the security assessment process and to enable CSPs to move through the assessment process as quickly as possible. You are allowed to make modifications to the templates as long as you don't remove any required sections. While the templates have been designed to capture the FedRAMP requirements, if adding new sections enables you to better describe your information system, it is acceptable to do that. Note that if you add new sections, the section numbering will change and some of the guidance found in this document refers to document section numbers. Therefore, changing the document section numbers might make it more difficult for you to use this document as a guide.

5.2 SENSITIVITY MARKINGS

Ensure that all documents have sensitivity markings on at least the cover page and the footer of each document. You may change the existing sensitivity marking on any template to match your official company sensitivity nomenclature if it is different than what is on the template. Optionally, you may also put your sensitivity markings on the headers of any documents and on any other places in the documents where you feel sensitivity markings should be placed. Any documents that do not have sensitivity markings on them could possibly be subject to a Freedom of Information Act (FOIA) request.

5.3 ITEMS THAT ARE NOT APPLICABLE

If you feel that a particular control requirement is not applicable to your system, do not leave the section in the template blank and do not delete that section. Simply write "Not Applicable" in that section. Be prepared to justify why any requirement is not applicable.